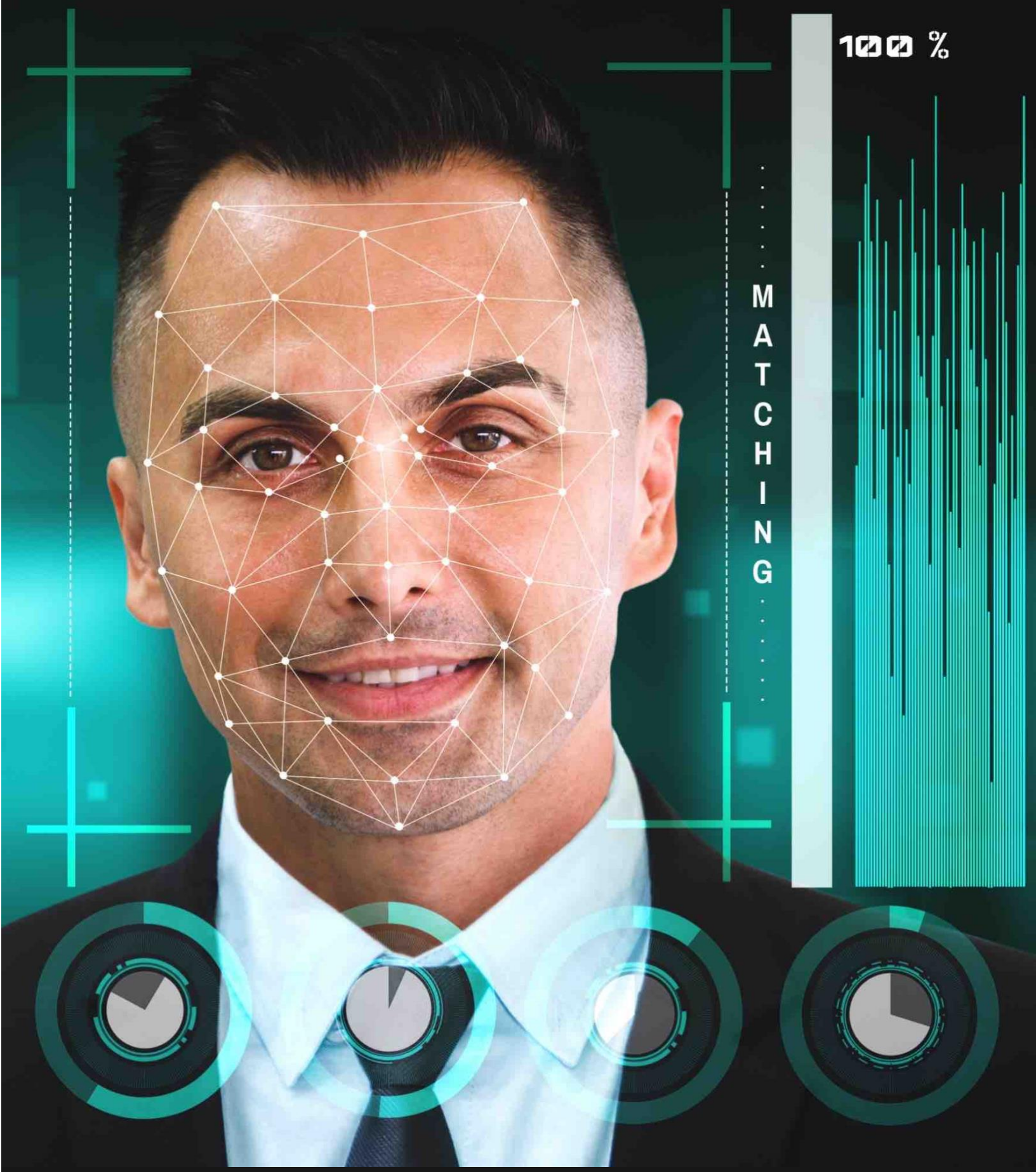

LEGAL BASICS OF REGULATION OF THE INFORMATION IN BULGARIA

George G. Dimitrov

LEGAL BASICS OF REGULATION OF THE INFORMATION IN BULGARIA

GEORGE G. DIMITROV

December 2023
Sofia

Publishing house:
Law and Internet Foundation

Author:
Prof. Dr. George Georgiev Dimitrov
University for Library Studies and Information Technologies, Sofia, Bulgaria
E-mail: george.dimitrov@netlaw.bg

Citation:
Dimitrov, G., Legal basics of regulation of the information in Bulgaria, Law and Internet Foundation, Sofia, 2023

ISBN 978-619-7192-23-0
First Edition. December 2023

THE AUTHOR

George Dimitrov holds a Doctor of Laws degree from the Katholieke Universiteit Leuven, Belgium (Ph.D., 2008). He obtained a master's degree in law with honors at the Sofia University "St. Kliment Ohridski", Faculty of Law (LL.M., 1995) and specialized in the Academy of American and International Law, Dallas, USA, as a recipient of the prestigious "Victor Folsom" scholarship (2002). He studied economics of the financial sector at the University of Delaware, BC and microcomputer engineering and programming at the Technical University, Sofia. He is currently a qualified teacher - professor of information and communication technology law at the University of Library Science and Information Technology. He teaches at the Sofia University "St. Kliment Ohridski", Plovdiv University "Paisii Hilendarski", Veliko Tarnovo University "St. St. Cyril and Methodius" and in the Center for the Training of Lawyers "Krastyu Tsonchev".

The author is a partner and founder of one of the leading Bulgarian law firms "Dimitrov, Petrov and Co." (www.dpc.bg) and is the chairman of the Supervisory Board. He is also the founder and chairman of the Board of Directors of the first provider of authentication services to build a private scheme for electronic identification in Bulgaria - Eurotrust Technologies AD. He is an arbitrator at the Czech Court of Arbitration for disputes related to domains of the European generic level ".eu", at the Court of Arbitration of the Bulgarian Chamber of Commerce. Prof. Dimitrov was a member of the Advisory Council on Electronic Communications, Postal Services, Information Society and Electronic Government to the Minister of Transport, Information Technologies and Communications and the Committee on Transport and Communications to the National Assembly. He was an advisor to the Deputy Speaker of the National Assembly, to the Chairman of the Commission on Internal Security and Public Order, to the Deputy Prime Minister and to the Minister of Justice in the Republic of Bulgaria. He was an advisor on electronic identification and authentication services to the Minister of Information Society and Administration of the Republic of North Macedonia.

In his capacity as chairman of the Law and Internet Foundation (www.netlaw.bg), Prof. Dimitrov was an expert and head of numerous working groups that developed modern Bulgarian legislation regulating public relations in the field of information and communication technologies, among which The e-Commerce Act, the e-Identification Act, the e-Government Act, the Electronic Communications Act, the Commercial Register Act, the Electronic Document and Electronic Authentication Services Act, the provisions of the Criminal Code governing computer crimes, the legislation governing e-justice and dozens

other legal and by-laws. He participated in the creation of strategies of key importance for the development of the information technology sector in Bulgaria, such as the Strategy for e-healthcare, the Strategy for e-governance, the Strategy for the competitiveness of Bulgaria in the global ICT markets, the Concept for the development of e-justice in Bulgaria, etc. .

He led the working groups at the Ministry of Information Society and the Administration of the Republic of North Macedonia, which developed the modern national regulatory framework, transposing the European framework for electronic identification and authentication services, as well as the regulation of electronic governance and registry reform.

Prof. Dr. Dimitrov was an expert for the working group on remote electronic identification for the needs of anti-money laundering measures at the European Commission and a national correspondent for Bulgaria on numerous international projects of the European Commission, the World Bank, the British Council and other international institutions. in connection with the implementation of European legislation in the field of personal data protection, electronic signatures, electronic documents, electronic commerce and electronic management.

For many years, Prof. Dr. Dimitrov has been training lawyers, judges, prosecutors, investigators, legal advisors and civil servants on the legal issues of information technology. He is the author of dozens of books and articles published in prestigious international publications. Member of the Editorial Board of "Digital Evidence and Electronic Signature Law Review". Lecturer and panelist in numerous national and international conferences, seminars and working groups.

He is a member of various professional organizations and committees of national and international importance, such as the International Bar Association (IBA), the Advisory Scientific Council to the research direction "Information and Communication Sciences and Technologies" at the Bulgarian Academy of Sciences, the Program for the Development of the Financial and Private Sector of the World Bank Institute, the Scientific Council of the European Privacy Institute, etc. A lawyer from the Sofia Bar Association, and for many years he was a member of the Council of the Bar and of the High Bar Council. Georgi Dimitrov holds a Doctor of Law from the Catholic University of Leuven, Belgium (Ph.D., 2008). He obtained a master's degree in law with honors at the Sofia University "St. Kliment Ohridski", Faculty of Law (LL.M., 1995) and specialized in the Academy of American and International Law, Dallas, USA, as a recipient of the prestigious "Victor Folsom" scholarship (2002). He studied economics of the financial sector at the University of Delaware, BC and microcomputer engineering and programming at the Technical University, Sofia. He is currently a qualified teacher - professor of information and communication technology law at the University of Library Science and Information

Technology. He teaches at the Sofia University "St. Kliment Ohridski", Plovdiv University "Paisii Hilendarski", Veliko Tarnovo University "St. St. Cyril and Methodius" and in the Center for the Training of Lawyers "Krastyu Tsonchev".

The author is a partner and founder of one of the leading Bulgarian law firms "Dimitrov, Petrov and Co." (www.dpc.bg) and is the chairman of the Supervisory Board. He is also the founder and chairman of the Board of Directors of the first provider of authentication services to build a private scheme for electronic identification in Bulgaria - Eurotrust Technologies AD. He is an arbitrator at the Czech Court of Arbitration for disputes related to domains of the European generic level ".eu", at the Court of Arbitration of the Bulgarian Chamber of Commerce. Prof. Dimitrov was a member of the Advisory Council on Electronic Communications, Postal Services, Information Society and Electronic Government to the Minister of Transport, Information Technologies and Communications and the Committee on Transport and Communications to the National Assembly. He was an advisor to the Deputy Speaker of the National Assembly, to the Chairman of the Commission on Internal Security and Public Order, to the Deputy Prime Minister and to the Minister of Justice in the Republic of Bulgaria. He was an advisor on electronic identification and authentication services to the Minister of Information Society and Administration of the Republic of North Macedonia.

In his capacity as chairman of the Law and Internet Foundation (www.netlaw.bg), Prof. Dimitrov was an expert and head of numerous working groups that developed modern Bulgarian legislation regulating public relations in the field of information and communication technologies, among which The e-Commerce Act, the e-Identification Act, the e-Government Act, the Electronic Communications Act, the Commercial Register Act, the Electronic Document and Electronic Authentication Services Act, the provisions of the Criminal Code governing computer crimes, the legislation governing e-justice and dozens other legal and by-laws. He participated in the creation of strategies of key importance for the development of the information technology sector in Bulgaria, such as the Strategy for e-healthcare, the Strategy for e-governance, the Strategy for the competitiveness of Bulgaria in the global ICT markets, the Concept for the development of e-justice in Bulgaria, etc. . He is a member of various professional organizations and committees of national and international importance, such as the International Bar Association (IBA), the Advisory Scientific Council to the research direction "Information and Communication Sciences and Technologies" at the Bulgarian Academy of Sciences, the Program for the Development of the Financial and Private Sector of the World Bank Institute, the Scientific Council of the European Privacy Institute, etc. A lawyer from the Sofia Bar Association, and for many years he was a member of the Council of the Bar and of the High Bar Council. Georgi Dimitrov holds a Doctor of Law from the Catholic University of Leuven, Belgium (Ph.D., 2008). He obtained a master's degree in law with honors at the Sofia University "St.

Kliment Ohridski", Faculty of Law (LL.M., 1995) and specialized in the Academy of American and International Law, Dallas, USA, as a recipient of the prestigious "Victor Folsom" scholarship (2002). He studied economics of the financial sector at the University of Delaware, BC and microcomputer engineering and programming at the Technical University, Sofia. He is currently a qualified teacher - professor of information and communication technology law at the University of Library Science and Information Technology. He teaches at the Sofia University "St. Kliment Ohridski", Plovdiv University "Paisii Hilendarski", Veliko Tarnovo University "St. St. Cyril and Methodius" and in the Center for the Training of Lawyers "Krastyu Tsonchev".

The author is a partner and founder of one of the leading Bulgarian law firms "Dimitrov, Petrov and Co." (www.dpc.bg) and is the chairman of the Supervisory Board. He is also the founder and chairman of the Board of Directors of the first provider of authentication services to build a private scheme for electronic identification in Bulgaria - Eurotrust Technologies AD. He is an arbitrator at the Czech Court of Arbitration for disputes related to domains of the European generic level ".eu", at the Court of Arbitration of the Bulgarian Chamber of Commerce. Prof. Dimitrov was a member of the Advisory Council on Electronic Communications, Postal Services, Information Society and Electronic Government to the Minister of Transport, Information Technologies and Communications and the Committee on Transport and Communications to the National Assembly. He was an advisor to the Deputy Speaker of the National Assembly, to the Chairman of the Commission on Internal Security and Public Order, to the Deputy Prime Minister and to the Minister of Justice in the Republic of Bulgaria. He was an advisor on electronic identification and authentication services to the Minister of Information Society and Administration of the Republic of North Macedonia.

In his capacity as chairman of the Law and Internet Foundation (www.netlaw.bg), Prof. Dimitrov was an expert and head of numerous working groups that developed modern Bulgarian legislation regulating public relations in the field of information and communication technologies, among which The e-Commerce Act, the e-Identification Act, the e-Government Act, the Electronic Communications Act, the Commercial Register Act, the Electronic Document and Electronic Authentication Services Act, the provisions of the Criminal Code governing computer crimes, the legislation governing e-justice and dozens other legal and by-laws. He participated in the creation of strategies of key importance for the development of the information technology sector in Bulgaria, such as the Strategy for e-healthcare, the Strategy for e-governance, the Strategy for the competitiveness of Bulgaria in the global ICT markets, the Concept for the development of e-justice in Bulgaria, etc.

He led the working groups at the Ministry of Information Society and the Administration of the Republic of North Macedonia, which developed the modern national

regulatory framework, transposing the European framework for electronic identification and authentication services, as well as the regulation of electronic governance and registry reform.

Prof. Dr. Dimitrov was an expert for the working group on remote electronic identification for the needs of anti-money laundering measures at the European Commission and a national correspondent for Bulgaria on numerous international projects of the European Commission, the World Bank, the British Council and other international institutions. in connection with the implementation of European legislation in the field of personal data protection, electronic signatures, electronic documents, electronic commerce and electronic management.

For many years, Prof. Dr. Dimitrov has been training lawyers, judges, prosecutors, investigators, legal advisors and civil servants on the legal issues of information technology. He is the author of dozens of books and articles published in prestigious international publications. Member of the Editorial Board of "Digital Evidence and Electronic Signature Law Review". Lecturer and panelist in numerous national and international conferences, seminars and working groups.

He is a member of various professional organizations and committees of national and international importance, such as the International Bar Association (IBA), the Advisory Scientific Council to the research direction "Information and Communication Sciences and Technologies" at the Bulgarian Academy of Sciences, the Program for the Development of the Financial and Private Sector of the World Bank Institute, the Scientific Council of the European Privacy Institute, etc. A lawyer from the Sofia Bar Association, and for many years he was a member of the Council of the Bar and of the High Bar Council.

Prof. Dr. George Dimitrov

LEGAL BASICS OF THE REGULATION OF INFORMATION IN BULGARIA

CONTENTS

LIST OF ABBREVIATIONS USED

SANS	State Agency “National Security”
SG	State Gazette
SCIS	State Commission on Information Security
AP	Additional provisions
EGN	Identification number
EU	European Union
AL	Administration Law
LSANS	Law on State Agency "National Security"
APIA	Access to Public Information Act
EDETSA	Electronic Document and Electronic Trust Services ACT
ECA	Electronic Communications Act
EGA	Electronic Governance Act
PDPA	Personal Data Protection Act
NAFA	National Archives Fund Act
SIMA	Special Intelligence Means Act
ICT	Information and Communication Technologies
Inspectorate	Inspectorate at the Supreme Judicial Council
CPPD	Commission for the Protection of Personal Data
CIS	Communication and Information Systems
CRB	Constitution of the Republic of Bulgaria
CRC	Communications Regulatory Commission
MEG	Minitry of Elecrtonic Governance
MI	Ministry of Interior
OMGCSAIS	Ordinance on the mandatory general conditions for the security of automated information systems or networks in which classified information is created, processed, stored and transferred
OCSCI	Ordinance on the cryptographic security of classified information
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the 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 repealing Directive 95/46/EC (General Regulation on Data Protection)
RILPCI	Regulations for the Implementation of the Law on the Protection of Classified Information
WG29	Working group for the protection of personal data under Article 29 of Directive 95/46

INTRODUCTION

This monograph aims to examine the information regime, in particular - the rules for the protection of the privacy of the personal sphere in electronic communications, the order for access to public information and the reuse of information from the public sector, as well as the rules for the protection of classified information – through the lens of Bulgarian legislation and European Union (EU) legislation.

Today's technologically advanced world deals with an ever-increasing amount of information, and its importance to modern societies is vital. This requires the person of the XXI century to have basic knowledge about the different types of information and the different normative rules and principles that regulate it. How is privacy guaranteed in electronic communications? What is "public information" and how is it accessed? What does "public sector use of information" mean? What information is "classified", what types of information are classified, and what rules are in place to protect it? The answer to these and other key questions about the information regime is given in this statement.

The monograph comprises of four chapters which cover the privacy of the electronic communications, the access to public information, the reuse of public sector information and the classified information.

This work is intended for international businesses who am at establish their business endeavors in Bulgaria. It can also be used by practicing managers, lawyers, economists, IT specialists, enterprise information management specialists and anyone interested in the regulation of the information in Bulgaria.

I. PRIVACY OF ELECTRONIC COMMUNICATIONS

The development of electronic communications necessitates the need for a new specific legal framework to protect the basic human rights of privacy and freedom without restricting the free movement and access to information. In this specific area, the main legal framework is laid down in Directive 2002/58/EC[1]on the right to privacy and electronic communications regarding the processing of personal data and protection of the right to privacy in the electronic communications sector[2]. This directive, as well as Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data created or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC (Directive 2006/24) have been implemented in Bulgarian law within the framework of the liberalization process in the telecommunications sector and at the moment the Electronic Communications Act (ECA) has been harmonized with their requirements. By a decision of the European Union dated 04/08/2014, part of the regulations applicable in this area (regarding the storage of traffic data) - in particular Directive 2006/24/ was

[1]Several other key legal acts complement the regulation in this matter. First, in 2015, Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures on access to the open internet and amending Directive 2002/22/EC on universal service and rights was adopted of users in relation to electronic communication networks and services and of Regulation (EU) No. 531/2012 on roaming in public mobile communication networks within the Union (text of EEA relevance), Pron. OJ L 310, 26.11.2015, p. 1–18. URL: <https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32015R2120&from=BG>. Second, in 2018, Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing a European Electronic Communications Code (Revised) (Text with EEA relevance) was adopted, Pub. OJ L 321, 17.12.2018, pp. 36–214. URL: <https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32018L1972&from=EN>

[2]At the EU level, a serious reform is currently being prepared, aimed at modernizing the legal framework in the field of privacy in electronic communications. A new legislative act - a regulation to replace Directive 2002/58 - the so-called ePrivacy Regulation, is under discussion. See more on the topic of Proposal for an ePrivacy Regulation. // EU. Strategy, Digital Single Market, POLICY, 19 June 2019. URL: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> (10.09.2019).

declared invalid[3]. As a result, the Bulgarian Constitutional Court adopted Decision No. 2 of 12/02/2015 of the Constitutional Court of the Republic of Bulgaria in Constitutional Case No. 8/2014, declaring the legal framework for storing traffic data unconstitutional. Directly after that, new legal texts were adopted in the EU and it is this legal regulation that should be analyzed.

1. Protection of electronic messages

The Constitution of the Republic of Bulgaria establishes that freedom and secrecyof correspondence are inviolable, and exceptions to this rule are allowed only with the permission of the judiciary when this is necessary for the detection or prevention of serious crimes.[4] Confidentiality of correspondence means that the information contained in the messages should be known only to the person sending it and the person to whom it is intended, until one of those persons decides otherwise.[5]

The WEC further develops this constitutional principle. One of the main goals and principles of the law is to help ensure a high level of personal data protection and privacy in the field of electronic communications.[6]

It can be argued that the protection of personal datain the case of electronic messages, it is a special case of personal data protection in general[7]. In this line of

[3]See Decision of the Court of Justice of the European Union in cases C-293/12 and C-594/12 of 8 April 2014 // Official Journal of the European Union, 10.6.2014, C 175/6-7. URL: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:62012CA0293&from=SV>. With it, the Court accepts that Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data created or processed in connection with the provision of publicly accessible electronic communications services or public communications networks and for amendment of Directive 2002/58/EC is incompatible in its entirety with Article 52(1) of the Charter of Fundamental Rights of the European Union, insofar as the resulting restrictions on the exercise of fundamental rights caused by the data retention obligation imposed by it do not are accompanied by mandatory principles aimed at regulating the necessary guarantees for regulating access to the specified data and their use. In view of the above, the Court sets aside the directives.

[4]Art. 34 CRB.

[5]See Decision No. 7982 of December 22, 2000 of the Supreme Administrative Court in Administrative Case No. 3351/2000.

[6]Art. 4 ECA.

[7]See Aleksandrov, A. New forms of employer control. Can the electronic correspondence of the staff be subject to control by the employer? // Labor and law, no. 4, April 2012, p. 17. See also Determann L. Sprague, R., Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States", 26 Berkeley Tech. LJ 979, 2011. URL: <http://scholarship.law.berkeley.edu/btlj/vol26/iss2/3> (24.10.2019).

thought, the provisions of the WEU appear special in relation to the general rules of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in relation to the processing of personal data and on the free movement of such data and for the repeal of Directive 95/46/EC (General Data Protection Regulation) (GDPR) and GDPR. ECA further develops and regulates the specifics of personal data protection for the purposes of providing electronic communication services and networks[8]. This is particularly clear in a new rule[9]of the ECA, created in 2019 as part of the amendments to synchronize the national legislation on the protection of personal data with the GDPR. According to this rule, enterprises providing public electronic communication services process lawfully collected personal data of users - natural persons, in accordance with the rules of the General Data Protection Regulation, and for issues not regulated therein - in accordance with the GDPR. In other words, in matters of personal data protection, the special rules of the European Union are leading, and only unsettled issues are regulated by the general regime of the GDPR and the GDPR.

The law stipulates a number of obligations for enterprises providing public electronic communication services and networks. They may not request from users more data than is expressly provided by law as a prerequisite for providing their electronic communication services and networks, unless the law provides otherwise or the service cannot be provided without the presence of other required data.[10]

1.1. Privacy of Messages

The privacy of electronic messages is the first element of the protection ofthe messages. It is guaranteed by the establishment of several rules.[11]

The law primarily establishes an obligation for enterprises providing public electronic communication networks and services not to disclose or distribute

[8]See Section III, Chapter Fifteen of the Law on Economic and Social Affairs.
[9]Art. 249, para. 3 ECA.
[10]Art. 249 ECA.
[11]See Section II, Chapter Fifteen of the Law of the European Union.

messages and related traffic data, location data, as well as the data necessary to identify the user, which became known to them in the process of their activity.[12]This obligation also applies to the employees of these enterprises who have or could gain access to such communications and information.

Restrictions do not apply to the recording of messages and related traffic data, when it is necessary and provided for by law in order to prove the conclusion of commercial transactions and when the sender and recipient of the messages are notified in advance of the recording, purposes and term of storage, as well as of the right to refuse this.[13]Such cases are the conclusion of contracts for the use of electronic communication services at a distance, customer service for changing the conditions for the use of services through a telephone customer service center and the like.

Secondly, the law establishes that the prohibition of interception of messages does not apply to enterprises providing electronic communication networks and services, when storage is required for technical reasons or is an essential part of the provision of the service, or a check of technical parameters is carried out of the service by authorized persons under the ECA. Examples can be many. If a new route or call quality is being tested for an exposed cell on a mobile network or the service is consumed through voice communication between the user and an automated system of the mobile operator, the limitations of the law will not apply. In such cases, however, the enterprises providing public electronic communication networks and services are obliged to delete the stored messages immediately after the reason for their storage ceases.[14]

1.2. Security of electronic communication networks and services

The second element of message security is connectedwith the security of electronic communication networks and services.

[12]Art. 245 ECA.
[13]Art. 247 ECA.
[14]Art. 246 ECA.

In Section I of Chapter 15 of the EU Law, entitled "Security and integrity of electronic communication networks and services", the obligation of enterprises providing electronic communication networks and services to take appropriate technical and organizational measures to manage the risk of network security and services providing an appropriate level of security, depending on the risk. The measures ensure a level of security commensurate with the existing risk, taking into account the nature of the problem and the costs of their implementation. These measures are aimed at preventing incidents and minimizing their impact on users and interconnected networks.[15]

Undertakings providing public electronic communications networks are also required to take all necessary actions to ensure the integrity of their networks and thus ensure the uninterrupted provision of services over those networks.

Security is expressed in ensuring such operating conditions of the networks and messages that do not allow their accidental or deliberate manipulation by third parties or by unauthorized employees of the enterprise, which would lead to the disclosure of the secret of the correspondence or to the thwarting of its transmission from the author to the addressee.

An important obligation of the WEC is imposed on enterprises providing public electronic communication networks and/or services in the event of a security breach or breach of integrity that has had a significant impact on the functioning of the networks or services. In these cases, businesses are required to notify the Communications Regulatory Commission (CRC) immediately. The logic of settling such a short period is that such adverse events are of a nature to significantly affect the interests of the public and consumers and this necessitates the immediate notification of the competent authority with supervisory powers with a view to taking follow-up measures.

Several consequences (legal possibilities, respectively obligations) arise from this notification for the CRC:

[15]Art. 243 ECA.

- First, the CRC can inform the public or require businesses to do so if it determines that it is in the public interest to disclose the breach. This decision is left to the discretion of the competent authority, which will take into account all the circumstances and possible harmful consequences of the case and assess whether such information is in the interest of society and consumers.
- Second, the CRC, at its discretion, may inform the competent national regulatory authorities of the affected member states of the European Union and the European Agency for Network and Information Security about these cases. This decision is again left to the discretion of the competent authority to consider whether other countries are affected and whether this requires notification of the competent authorities of those other countries and/or notification of the competent European authorities.
- Third, the CRC must inform the Minister of Transport, Information Technologies and Communications and the National Computer Security Incident Response Team, established pursuant to Art. 19, para. 1 of the Cyber Security Act for these cases. There is no room for judgment here and this is imputed as an obligation of the CRC.
- Fourth, once a year the CRC must submit to the European Commission and the European Network and Information Security Agency a summary report of the received notifications of security breaches or breaches of integrity that have had a significant impact on the functioning of networks or services, as well as actions taken.

In addition to the above, the CRC has the authority to require enterprises providing public electronic communications networks and/or services to: (1) provide information necessary to assess the security and/or integrity of their services and networks, including documented security policies, and (2) subject the security to an audit performed by a qualified independent body and provide the results of the audit to the CRC. In these cases, the law stipulates that the costs of the audit are to be borne by the enterprise concerned. CRC can also give mandatory instructions, including deadlines for implementation, to these enterprises to take specific measures to ensure the security of the networks and the services provided through them.

In the event of a risk of breaching the security of electronic communication networks, the enterprise should notify its subscribers in an appropriate manner of the risk, of the necessary means for its removal, as well as of the related costs.[16]

1.3. Protection of user data

The third element of the protection of electronic messages is expressed in the provision of rules and tools for the protection of users' data.

The law restricts enterprises providing public electronic communication networks and services, including networks supporting data collection and identification devices in this direction. They can process data of end users only when these data are directly intended for the provision of electronic communication services such as name, social security number, address, etc.

Enterprises providing public electronic communication services cannot set conditions for the provision of their services depending on the user's consent for their data to be used for other purposes.[17]Attempts to circumvent this rule are unfortunately common - the right of enterprises to use the data for other purposes is usually set out in the General Terms and Conditions of use of certain electronic communication services or in their annexes and the user is put in a situation or to accept the entire general terms and conditions , together with the consent to have his data processed, or not to enter into a contract. Such an approach is vicious and contrary to the spirit of the law. Insofar as the law imposes special requirements and restrictions on the purposes for which the data can be processed, in some cases the inclusion of certain consents in the general conditions cannot guarantee the existence of a valid consent with their acceptance by the user. In addition, there are also a number of mandatory prescriptions from the CPPD and the CRS aimed at limiting such improper practices. Last but not least, the requirement of such

[16]Art. 244 ECA. Specific obligations for filtering certain types of content are also provided for under the Cybersecurity Act - see Art. 14, para. 5, Art. 15, para. 6 and Art. 19, para. 3.
[17]See Art. 249 ECA.

consent, which is made dependent on the provision of the service, in light of the new GDPR rules, is invalid[18].

As already mentioned, the enterprises providing public electronic communication services and networks are obliged not to disclose and not to distribute the data necessary to identify the user, which became known to them during the provision of electronic communication networks and services.[19]

The legislator has established special rules regarding the protection of the following three groups of user data.

*The first set of data*covers the so-called "traffic data". These are:

- number of calling and called end user, electronic payment card number;
- start and end of the call, determined by date and time, accurate to the second if technical possibility exists and/or in the case of data transfer - volume of transferred data, for billing purposes;
- type of service provided;
- points of mutual connection when making the call, beginning and end of their use, determined by date and time, accurate to the second if technically possible;
- data on the type of connection or zones - hourly and territorial, necessary to determine the value of the service;
- location of a user of a service provided by a mobile network, including when providing the "roaming" service.

The second group covers the data necessary to prepare the subscriber accounts, as well as to prove their credibility, such as:

- subscriber data: for natural persons – the three names, uniform civil number and address, and for foreign persons – personal number; for legal entities and individuals - sole traders - name, registered office, management address and relevant identification code;
- type of electronic communication services used;

[18]See Working Party on the Protection of Personal Data under Article 29. Guidance on Consent in accordance with Regulation 2016/679, adopted on 28 November 2017, last revised and adopted on 10 April 2018, WP259 rev.01.
[19]Art. 245 ECA.

- total number of units of measurement charged for the relevant period of preparation of the bill in the case of a periodic bill;
- value of the services used for the relevant period;
- information related to the payment method chosen by the subscriber and the payments made and due;
- information about changes in the use of the service - restriction of use, removal of restriction.

*The third group*data affecting the user's location. This is data that is processed in electronic communication networks to determine the geographic location of the end user's electronic communication device.

The protection of the above groups of data is expressed in limiting the ability of enterprises providing public electronic communication networks and services, including networks supporting data collection and identification devices, to process this user data only when it is directly intended for the provision of electronic communication services.

Enterprises providing public electronic communication services may collect, process and use user data[20]and for other purposes, such as:

- detection, localization and elimination of malfunctions and software errors in electronic communication networks;
- detection and cessation of illegal use of electronic communication networks and facilities, when there is reason to believe that such actions are taking place and this is stated in writing by the affected party or a competent authority;
- detection and tracking of nuisance calls in the presence of a request from the affected subscriber, requiring measures to be taken by the enterprise offering the service.[21]

[20]It is about the data under Art. 248, para. 2 ECA.
[21]Art. 256 ECA.

1.4. Traffic data

Art. 250 ZE regulates a special regime in relation to traffic data and creates certain obligations for enterprises providing public electronic communication networks or public electronic communication services.

Traffic data is any information related to electronic messages, but not their content. According to Art. 248, para. 2, item 1 ECA traffic dataare the data necessary for the provision of electronic communication services, for billing, for forming the accounts of the subscribers, as well as for proving their credibility (i.e. the above-mentioned first group of data).

Separately, a legal definition is also contained in § 1, item 71 AP of ECA, according to which "traffic data" "is data processed for the purpose of transmitting a message over an electronic communication network or necessary for its billing." This legislative approach is inconsistent and creates ambiguity and potential confusion for the law's addressees. It is recommended that de lege ferenda in the WEU have a single definition of "traffic data".

Enterprises providing public electronic communication services that collect, process and use traffic datafor the purposes of a given call or making a connection, are obliged after the call or connection to delete this data or to depersonalize it, unless it is immediately necessary to make a new call or in the cases provided by law. Undertakings providing public electronic communications services must also provide users with accurate and complete information about the type of traffic data processed for the purposes of subscriber billing and interconnection payments and the duration of such processing.

After obtaining prior consent from users, they are entitled to provide traffic data, related to users, for the purpose of providing value-added services requiring additional processing of traffic data or location data other than the traffic data necessary to carry the message or to charge for it.[22]

[22]Art. 250 ECA.

In addition, the WEC obliges enterprises providing public electronic communication networks and/or services[23], to store data for a period of 6 months[24], created or processed in the course of their activity, which are necessary for:

- tracking and identifying the source of the link;
- identifying the direction of the connection;
- identification ofthe date, time and duration of the connection;
- identification ofthe type of connection;
- identification of the user's terminal electronic communications device or what appears to be the user's terminal device;
- establishment ofidentifier of the used cells.

This data is stored for the needs of national security and for the prevention, detection and investigation of serious crimes, including for the purposes of preventing serious crimes within the framework of operational-investigative activities in accordance with Chapter Nine of the Anti-Corruption Act and for confiscation of illegally acquired property. The data for establishing the identifier of the cells used are also stored for carrying out search and rescue operations in the cases under Art. 38, para. 3 of the Disaster Protection Act. ECA prohibits other data, including those revealing the content of messages, to be stored in this order. The specified categories of data are processed and stored in accordance with the requirements for the protection of personal data[25].

After the expiration of the specified six-month period, the enterprises providing public electronic communication networks and/or services are obliged to destroy the data and by every fifth of the month to provide the CPPD with a protocol for the data destroyed in the previous month. CPPD creates and maintains a register of provided protocols, which is not public. CPPD is authorized by the EU to carry out checks on the legality of the storage and destruction of data by enterprises[26].

[23]Art. 251b ECA.
[24]See Decision No. 2 of 12.02.2015 of the Constitutional Court of the Republic of Bulgaria pursuant to k. e. No. 8/2014, by which the old version of the Law on Law (Art. 250a - Art. 250e, Art. 251 and Art. 251a Law on Law), providing for a 12-month period for storing traffic data, was declared unconstitutional.
[25]The procedure for providing this information is described in Art. 251c – 251i ECA.
[26]See also Art. 261a ECA, which declares the CPPD as a supervisory authority regarding the security of data stored pursuant to Art. 251b, para. 1 ECA.

2. User's rights

The EU Law also regulates inviolability as part of consumer rights. The rules are very close to those provided for in the matter for the protection of personal data, but at the same time reveal some peculiarities. The right to the protection of personal data is governed by the GDPR and the GDPR, which only apply to natural persons and not to legal entities, while the provisions of the EU General Data Protection Regulation protect subscribers and end users, i.e. individuals and legal entities. However, according to Art. 262 EGA, the supervision of the processing of personal data according to the order of chapter fifteen, section III of the EGA is carried out by the GDPR in accordance with the GDPR and the GDPR.

Art. 21 WEC postulates that the functions of regulation and control in the implementation of electronic communications are carried out by the CRC. It is the competent authority that examines complaints of end users in the cases provided for in the Law of the Territories.[27]However, the CRS has the power to impose sanctions, but not to void/terminate contracts or order the return of overpaid accounts. These matters are within the competence of the civil court.

Special rules for the protection of user data are regulated by the General Requirements of the CRC for the implementation of public electronic communications (the General Requirements). They provide for various protective mechanisms for end users of electronic communication services - such as: how to notify end users of changes in general terms and conditions and in individual contracts; how to write part of the more essential clauses of the contracts such as penalties, termination conditions and others (eg with bold, font size at least 10 points, etc.), how to format the signature fields, the signing options of contracts with electronic signatures and a number of others.

The general requirements further develop the criteria for the impact assessment, the required information, the form and method of notification when a

[27]Art. 30, item 26 ECA.

security breach or breach of integrity that has had a significant impact on the operation of networks or services.

3. Trends in the development of the EU framework of privacy in electronic communication and its impact on the Bulgarian legislation

In the digital era, the privacy of electronic communications has become a paramount concern. With the pervasive use of the internet and mobile technologies, vast amounts of personal data are transmitted daily, making privacy a critical issue. The EU recognizes this and has actively worked to safeguard the privacy and data of its citizens. The significance of privacy in electronic communications stems from its direct impact on individual rights, including the right to privacy, freedom of expression, and protection from unwarranted surveillance. This has led to an increasing demand for robust regulatory frameworks to ensure that personal information is handled responsibly, securely, and transparently.

The EU has been a global leader in setting standards for data protection and privacy. Its approach to privacy regulation, especially in the context of electronic communications, has set a benchmark worldwide, influencing other regions and international policies. The EU’s legislative framework is designed to provide comprehensive protection to individuals regarding the processing of personal data, ensuring that personal information is not misused or exploited. This leadership role stems from the EU's commitment to uphold fundamental rights and freedoms, a commitment that is deeply rooted in its legal and cultural heritage. By prioritizing the protection of personal data, the EU plays a crucial role in shaping global norms and practices in the digital age.

Over the years, the EU's privacy regulations have evolved to keep pace with technological advancements and the changing landscape of electronic communications. This evolution reflects a proactive approach to addressing emerging challenges and threats to personal privacy in the digital sphere. The regulations have expanded in scope, covering various aspects of electronic

communications, from general data protection laws to specific directives targeting online communications and digital marketing. The dynamic nature of these regulations indicates the EU's commitment to continually updating and refining its legal frameworks to protect citizens' privacy effectively in an increasingly interconnected world. As a result, the EU's privacy regulations are not only comprehensive but also forward-looking, anticipating future challenges and adapting to the ever-changing digital landscape.

3.1. Trends in regulation of VoIP services and privacy

Voice over Internet Protocol (VoIP) services, which enable voice and multimedia communication over the internet, have become integral to modern communication. However, their rise has brought unique challenges in the realm of privacy regulation.[28] The European Union (EU) has been particularly proactive in addressing these challenges, recognizing that traditional telecommunication regulations might not fully encompass the nuances of internet-based communication services.

The need for explicit protection of VoIP communications arises from the distinct nature of data transmitted over these services. Unlike traditional telephony, VoIP not only transmits voice but also potentially exposes sensitive data like IP addresses and call logs, creating new avenues for privacy breaches. The EU's regulatory approach towards VoIP services thus focuses on safeguarding personal data and ensuring confidentiality of the communications. This includes the protection against unauthorized access and processing of personal data, as well as providing users with clear information about data usage and consent options.

Another significant aspect of the EU's regulation is ensuring interoperability and security standards among VoIP service providers. This is crucial for maintaining the integrity and confidentiality of communications. The EU's General Data Protection Regulation (GDPR), for instance, plays a critical role in this context. GDPR's stringent data protection requirements compel VoIP providers to

[28] R. Wong & Daniel B. Garrie on Regulation of VoIP Services and Privacy: Wong, R., & Garrie, D. B. (2009). Regulation of VoIP Services: Bridging the Gap Between Traditional Telephony and Electronic Communications (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1466153).

implement robust security measures and offer transparency regarding data processing practices. The regulation also grants individuals greater control over their personal data, aligning with the EU's broader commitment to privacy and data protection.

The EU's regulatory framework for VoIP services is a testament to its commitment to adapt and respond to technological advancements in communication. By extending privacy and data protection norms to encompass VoIP services, the EU ensures that privacy rights are upheld in the evolving landscape of digital communication.

3.2. Fragmentation in European privacy law and policy

European privacy law and policy, particularly in the field of electronic communications, have been characterized by a certain degree of fragmentation.[29] This fragmentation is primarily due to the diverse approaches taken by different EU member states in implementing EU directives and regulations. Each country's unique legal, cultural, and historical contexts have influenced how these laws are applied, leading to a patchwork of privacy standards across the region.

One of the critical issues arising from this fragmentation is the lack of a unified approach to privacy and data protection. While the EU has established overarching frameworks like the GDPR and the e-Privacy Directive, their interpretation and enforcement can vary significantly across member states. This variation poses challenges for businesses operating across borders, as they must navigate differing privacy requirements in different jurisdictions. It also creates a complex environment for citizens, who may not have a clear understanding of their rights and protections under varying national laws.

The EU has recognized this issue and has made efforts to harmonize privacy laws across member states, but the process has been gradual. The complexity of reconciling different legal systems and the need to respect national sovereignty

[29] J. Hoboken on Fragmentation in European Privacy Law and Policy: Hoboken, J. (2014). European Privacy Law and Policy: A Critical Assessment. (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418636).

make this a challenging task. Despite these challenges, the EU continues to strive for a more cohesive and harmonized approach to privacy regulation. Such efforts are crucial in creating a stable and predictable legal environment for both individuals and businesses, and in maintaining the integrity of the single market.

In summary, while the EU has made significant strides in protecting privacy in electronic communications, the current state of European privacy law is still marked by fragmentation. The EU faces the ongoing challenge of balancing the need for harmonization with respect for the diverse legal traditions of its member states. Addressing this fragmentation is essential for ensuring effective and uniform privacy protection across the EU.

3.3. Regulation of digital networks and services in the EU

EU has been proactive in regulating digital networks and services, striving to create a comprehensive framework that caters to the rapidly evolving digital landscape. This regulatory approach is not just about enforcing privacy and data protection laws but also about stimulating private investment and innovation in digital infrastructure, particularly crucial in the era of 5G technology.

Key recommendations made by experts in the field, like Alexandre de Streel and P. Larouche, suggest a need to streamline and focus digital networks regulation.[30] This includes simplifying the regulatory environment to encourage private investment in digital networks. Such investments are essential for the advancement and rollout of next-generation networks, including 5G, which are pivotal for the EU's digital economy.

Another significant aspect of the EU's approach is the enhancement of spectrum policy coordination. Efficient and coordinated spectrum management is vital for the successful deployment of 5G networks across EU member states. This

[30] Alexandre de Streel & P. Larouche on Regulation of Digital Networks and Services: de Streel, A., & Larouche, P. (2016). Digital Networks and Services: A Specific Regulatory Framework (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728874).

not only supports the growth of the digital economy but also ensures a cohesive and integrated digital market across the EU.

Moreover, the creation of a framework for digital services based on general EU rules, such as privacy and data protection law, is another critical recommendation. This framework aims to balance the fast-paced innovation in digital services with the need to protect user privacy and data. It encompasses various digital services, including cloud computing, social media, and e-commerce, ensuring that they operate within a set of standardized, EU-wide regulations.

In essence, the EU's regulation of digital networks and services represents a balanced approach that seeks to foster innovation and investment while upholding stringent privacy and data protection standards. This approach is crucial in maintaining the EU's competitive edge in the global digital economy and in ensuring the protection of its citizens' digital rights.

3.4. Overview on the trends in EU regulation of privacy in electronic communications

The analysis of the EU regulatory trends in privacy and electronic communications reveals a comprehensive, adaptive, and forward-looking approach, addressing the complexities of the digital age. These regulations, evolving alongside technological advancements and societal needs, demonstrate the EU's commitment to safeguarding personal data and privacy in an interconnected world.[31]

Firstly, the EU's leadership in global data protection standards is evident. Through regulations such as the GDPR and the e-Privacy Directive, the EU has set a benchmark for privacy and data protection that influences global digital practices. These regulations reflect an understanding that privacy is not just a regulatory requirement but a fundamental right. The GDPR, in particular, has

[31] Alexandre de Streel & Christian Hocepied on EU Regulation of Telecommunications Networks and Services: Streel, A. D., & Hocepied, C. (Reference Year Not Available). EU Regulation of Electronic Communications Networks and Services (https://china.elgaronline.com/edcollchap/edcoll/9781786439321/9781786439321.00013.xml).

become a global model for data protection laws, emphasizing user consent, data minimization, and transparency.

Secondly, the EU's approach to addressing specific challenges posed by new technologies, such as VoIP services and smartphone data tracking, showcases its ability to adapt to changing communication landscapes. The proposed ePrivacy Regulation, for instance, represents a significant step in enhancing privacy protections in a world where digital tracking and data collection are prevalent. It shows the EU's keenness to balance the benefits of technological innovation with the imperative of protecting individual privacy.

Finally, the EU's efforts to harmonize privacy laws across member states, despite the challenges of legal and cultural diversity, are crucial for creating a stable and predictable environment for both individuals and businesses. The attempt to reduce fragmentation and bring about a more cohesive approach underlines the EU's commitment to a unified digital market where privacy and data protection are uniformly upheld.

In conclusion, the EU's regulatory framework for privacy in electronic communications is a dynamic and multifaceted response to the challenges and opportunities of the digital era. It not only ensures robust protection of personal data and privacy but also positions the EU as a global leader in the formulation of digital privacy standards. These efforts are integral to fostering trust and security in digital communications, essential components of a thriving digital economy and society.

II. ACCESS TO PUBLIC INFORMATION

1. Concept of access to public information

Mechanisms for the functioning of civil society require provision and guaranteecitizens of tools for civil control over the activity of the administration and all public institutions. The right to access information is an emanation of the principles enshrined in Art. 19 of the Universal Declaration of Human Rights and Art. 6, 8 and 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the UN Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters.[32]

The state apparatus of bodies assists in realizing the rights and legitimate interests of citizens. It cannot function in secret - on the contrary. What he creates in his activity as documents and information must be transparent and accessible to the public. The right of access to this information and to official documents in which it is contained provides a source of information for the public, helps citizens to form an opinion about the state of society and about government institutions, and supports the integrity, effectiveness, efficiency and accountability of public institutions , thereby strengthening their legitimacy.[33]

In this regard, the principle is established that all official documents are, as a rule, public and access to them can be denied only if the rights and legitimate interests of other persons will be affected in this way.[34]

The right of access to public informationis enshrined in many international acts.[35]In Bulgaria, it has found its legal protection in the Law on Access to Public Information(DSOI).[36]

---

[32]Adopted at Aarhus, Denmark on 25 June 1998.
[33]§5-7 of the European Convention on Access to Official Documents, adopted by the Committee of Ministers on 27 November 2008 at the 1042nd meeting of the Ministerial Plenipotentiaries.
[34]Tsekov, B. Access to public information. // Weekly Legalist, no. 31, July 31-August 6, 2000, pp. 1-2.
[35]See Regulation No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 on public access to European Parliament, Council and Commission documents, Charter of Fundamental Rights of the European Union (2007/C 303/01), European Convention on access to official documents, Recommendation (2002)2 of the

Public information in the sense of the law is any information related to public life in the Republic of Bulgaria and enabling citizens to form their own opinion regarding the activities of entities obligated by law.[37]

It is legally irrelevant on what material medium the information is objectified - it is public, regardless of its medium.[38]

Information that would affect the personal data of other persons cannot be requested. For access to them, the GDPR and the rules in the Bulgarian national legislation apply, in particular - the GDPR.

2. Subjects of the right of access to public information

Recipients of the obligation to provide accessto public information are several groups of persons who create or store public information.

First of all, these are the state bodies, their territorial units and local self-government bodies. The law practically covers all bodies in the state, including independent bodies such as the President, the National Assembly, the Audit Chamber, the Electronic Media Council, the Communications Regulatory Commission, etc.

Committee of Ministers to Member States on access to official documents, Recommendation R(2000)13 on European policy on access to archives, Recommendations R(81)19 and Recommendation R(94)13 of the Committee of Ministers of the Council of Europe, etc.

[36]Pron. SG. No. 55 of July 7, 2000, amended. SG. No. 1 of January 4, 2002, amended. SG. No. 45 of April 30, 2002, amended. SG. No. 103 of December 23, 2005, amended. SG. No. 24 of March 21, 2006, amended. SG. No. 30 of April 11, 2006, amended. SG. No. 59 of July 21, 2006, amended. SG. No. 49 of June 19, 2007, amended. SG. No. 57 of July 13, 2007, amended. SG. No. 104 of December 5, 2008, amended. SG. No. 77 of October 1, 2010, amended SG. No. 39 of May 20, 2011, amended and add. SG. No. 97 of December 11, 2015, amended SG. No. 13 of February 16, 2016, amended. and add. SG. No. 50 of July 1, 2016, amended SG. No. 85 of October 24, 2017, amended and add. SG. No. 77 of September 18, 2018, amended SG. No. 17 of February 26, 2019

[37]Thus, the concept of "public information" should be perceived as information, knowledge about someone or something related to public life in the country. This public information may be contained in documents or other material media created, received or stored by the subjects obliged under the FDSO. Decision No. 3327 of March 15, 2010 of the Supreme Administrative Court under Adm. e. No. 7481/2009

[38]Art. 2, para. 2 APIA. The information is public, regardless of the type of its material carrier – paper, electronic or other, and may be stored including on a sound or video recording. However, this does not constitute grounds for an authority under Art. 3 of the APIA to be charged with an obligation to allow access to a building to natural persons, necessary for the fulfillment of their personal goals. Decision No. 2008 of February 16, 2010 of the Supreme Administrative Court under Adm. e. No. 4930 / 2009

Next, these are all public law entities, other than the specified bodies, including public law organizations. A legal entity is considered to be such a legal entity for which any of the following conditions are met:

- more than half of its income for the previous budget year is financed from the state budget, from the budgets of the state social insurance or the National Health Insurance Fund, from the municipal budgets or from the President of the Republic of Bulgaria; by the Speaker of the National Assembly; the Prime Minister; the ministers; the Ombudsman of the Republic of Bulgaria; the governor of the Bulgarian National Bank; the president of the Constitutional Court of the Republic of Bulgaria, the administrative heads of the bodies of judicial power that manage independent budgets, as well as the administrative heads of the prosecutor's offices in the country; regional governors; the mayors of municipalities, regions, town halls, as well as the deputy mayors, when they are in charge of the budget; by the heads of state agencies; the chairmen of the state commissions; executive directors of executive agencies; the heads of state institutions established by law or by a decree of the Council of Ministers, including separate structures of the bodies of the executive power, when they are legal entities and disposers of the budget; from the representatives of public law organizations[39];
- more than half of the members of its management or control body are appointed by the President of the Republic of Bulgaria; by the Speaker of the National Assembly; the Prime Minister; the ministers; the Ombudsman of the Republic of Bulgaria; the governor of the Bulgarian National Bank; the president of the Constitutional Court of the Republic of Bulgaria, the administrative heads of the bodies of judicial power that manage independent budgets, as well as the administrative heads of the prosecutor's offices in the country; regional governors; the mayors of municipalities, regions, town halls, as well as the deputy mayors, when they are in charge of the budget; the heads of state agencies; the chairmen of the state commissions; executive directors of

[39]APIA defines these persons as "contractors under Art. 5, para. 2, items 1 – 14 of the Law on Public Procurement" (author's note).

executive agencies; the heads of state institutions established by law or by a decree of the Council of Ministers, including separate structures of the bodies of the executive power, when they are legal entities and disposers of the budget; from the representatives of public law organizations;

- is subject to management control by the President of the Republic of Bulgaria; the Speaker of the National Assembly; the Prime Minister; the ministers; the Ombudsman of the Republic of Bulgaria; the governor of the Bulgarian National Bank; the president of the Constitutional Court of the Republic of Bulgaria, the administrative heads of the bodies of judicial power that manage independent budgets, as well as the administrative heads of the prosecutor's offices in the country; regional governors; the mayors of municipalities, regions, town halls, as well as the deputy mayors, when they are in charge of the budget; the heads of state agencies; the chairmen of the state commissions; executive directors of executive agencies; the heads of state institutions established by law or by a decree of the Council of Ministers, including separate structures of the bodies of the executive power, when they are legal entities and disposers of the budget; from the representatives of public law organizations.Management control is present when one person can in any way exercise a dominant influence on the activity of another person.

A public-law organization is also a medical facility - a commercial company, where more than 50 percent of the revenues for the previous year are at the expense of the state and/or municipal budget and/or the budget of the National Health Insurance Fund.

A public organization is also a library of higher education institutions, a public library within the meaning of the Law on Public Libraries, a museum or an archive, the activity of which is financed with funds from the state budget or municipal budgets.

Thirdly, these are individuals and legal entities only regarding their activities, financed with funds from the consolidated state budget and with funds

from European Union funds or provided by the European Union under projects and programs. This is understandable - society's interests in publicity and transparency require the possibility of access to information stored by a larger group of persons, including private ones.

Empowered to request right of access to public informationare all citizens of the Republic of Bulgaria, foreigners, stateless persons and legal entities. The right is exercised according to the order of the Federal Data Protection Act, unless another law provides for a special order for searching, receiving and distributing such information.

3. Basic principles

The main principles in implementing the right of access to public information are referred to in Art. 6, para. 1 APIA. They are:

- openness, credibility and completeness of information;
- ensuring equal conditions for access to public information;
- ensuring legality in seeking and receiving public information;
- protection of the right to information;
- protection of personal data;
- ensuring the security of society and the state.

The right of access to public information, although not subject to restrictions, has its limits. Its boundaries extend to the rights and interests of other citizens or a secret protected by law. For example, a right of access to public information cannot be claimed when it is classified information, banking secrets, insurance secrets, personal data or other secrets protected by law. In addition, the exercise of the right of access to public information cannot be directed against the rights and good name of other persons, as well as against national security, public order, citizens' health and morals.

Outside the scope of the right of access to public information remains information that is provided in connection with the administrative service of citizens and legal entities or that is stored in the National Archive Fund of the

Republic of Bulgaria. The legislator's logic regarding limiting the possibility of obtaining access to information that is provided in connection with the administrative service of citizens and legal entities is based on the understanding that by exercising their administrative rights, individuals satisfy their legal interests. But the exercise of these rights is granted only to persons for whom the right has arisen on the basis of law. No other person could request and receive information about administrative proceedings and the data and documents created on the basis of it, which do not affect his right, but the right of a third party. In this sense, the rights of the third party have priority over the right of access to public information, and information on individual administrative proceedings is not public. With regard to the information concerning the National Archive Fund, there is a special procedure for providing it, defined in the Law on the National Archive Fund (NAAF).

Access to public information can be full or partial. This means that the subjects of the right of access can request the entire collected information or only a part of it for which they have a legal interest in knowing it. It is up to the entities to what extent they request this information.

4. Types of public information

The law differentiates two types of public information, created and stored by the authorities and their administrations:

- official and
- unofficial.

Official public information is that which is contained in the acts of state bodies and local self-government bodies in the exercise of their powers.

All acts issued by the authorities within their powers are taken into account - individual, general and normative.

Official information is information that is collected, created and stored in connection with official information, as well as in connection with the activities of the authorities and their administrations.

This information is not objectified in specific acts, but can be collected, stored and processed in various information systems (for example, administrative information systems in the sense of the Ordinance on the exchange of documents in administrations, in specialized information systems, etc.), stored on various paper media (registers, data sets) or contained in documents.

5. Access to public information

5.1. Access to official public information

The access to official information whichis contained in normative acts, is ensured through their promulgation. Access to other official information, in cases where this is provided for by law or by decision of the body that created it, is provided through publication.

Access to official information, outside of these cases, is free and is carried out in accordance with the rules of the Federal Data Protection Authority.

When requesting access to official information that has been promulgated, the relevant authority is obliged to indicate the edition in which it was promulgated, the number of the State Gazette and the date of publication.[40]

5.2. Access to official public information

Access to official public informationis free. Free means that any person can request the information and their access cannot be restricted, and the information can be selected at the authority's discretion. There may be a restriction on certain official public information only exceptionally, when it is (1) related to the operational preparation of the bodies' acts and has no independent significance

[40]See Art. 13, para. 1 APIA.

(opinions and recommendations prepared by or for the body, opinions and consultations) or (2) contains opinions and positions in relation to current or upcoming negotiations conducted by the body or on its behalf, as well as information related to them, and is prepared by the administrations of the relevant bodies. This is because in the process of making management decisions, economic interests often depend on the decisions of administrative bodies (especially in the field of public procurement, tenders, concessions, changes to building plans, etc.) and it is possible, in order to to obtain favorable information about one or other facts, for example within the framework of an open tender for granting a license to build a mobile communication network and provide mobile services - to give an economic advantage to some entities over others.

This limitation cannot be eternal. The legislator has considered that the public interest requires that, after a certain period of time has passed since the creation of such information (2 years), access should be free again.

However, no public information shall be provided which constitutes a trade secret and the provision or dissemination of which would lead to unfair competition between traders.[41]When refusing access to such information, the obliged entities are obliged to indicate the circumstances that lead to unfair competition between traders.

In all the cases listed above, access cannot be restricted in the presence of the so-called "overriding public interest", defined in § 1, item 6 of the Additional Provisions (AP) of the Supplementary Regulations.

There is an overriding public interest when, through the requested information, the aim is to reveal corruption and abuse of power, to increase the transparency and accountability of the entities obliged under the PDOI.

In these cases, the interests of society take precedence over the interests of the entities that may be affected by its provision.

[41]Art. 17 APIA.

5.3. Provision and publication of public information

For purposes of transparency and civil controlon the activity of the state and local bodies is the statutory obligation established in their burden to inform the public about their activity through publication or communication in another form.

The obligation to inform covers information collected or made known to them in the course of their activities, when this information:

- can prevent a threat to the life, health and safety of citizens or their property;
- refutes disseminated false information affecting significant public interests;
- represents or would represent a public interest;
- should be prepared or provided by operation of law.

For example, for industrial accidents or events of public importance, the authorities are obliged to publicize the collected information by publishing it in daily newspapers or other forms of periodicals, in the electronic media, convening press conferences and other appropriate forms. The methods are not exhaustively listed - they are left to the authority's discretion.

Again, in order to ensure transparency in the activity of the administration and to maximally facilitate access to public information, a specific obligation has been imposed on certain groups of addressees - the heads of administrative structures in the executive power system - to periodically publish up-to-date information containing:

- a description of their powers and data on the organization, functions and responsibilities of the administrations they lead;
- a list of the acts issued in fulfillment of their powers and the texts of the normative and general administrative acts issued by the body;
- description of the information arrays and resources used by the respective administrations;
- the name, (physical) address, the e-mail address, telephone number and working hours of the unit in the relevant administrations responsible for accepting applications for granting access to information;

- by-laws and internal rules related to the provision of administrative services to citizens;
- strategies, plans, programs and activity reports;
- information on the budget and financial statements of the administration, which is published according to the Law on Public Finances;
- information about conducted public procurements, determined to be published in the buyer's profile according to the Law on Public Procurements;
- drafts of normative acts, together with the reasons, respectively – the report and the results of the public discussion of the project;
- notifications for the opening of the proceedings for the issuance of a general administrative act under Art. 66 of the Administrative Procedure Code, including - the main considerations for the issuance of the act and the forms and terms of participation of the interested persons in the proceedings;
- information on the exercise of the right of access to public information, on the terms and conditions for reuse of information, on the fees under Art. 41g APIA and the formats in which the information is maintained;
- announcements for competitions for civil servants;
- information subject to publication under the Law on Prevention and Identification of Conflict of Interest;
- information that is public, according to the Law on the Protection of Classified Information and the acts on its implementation;
- the information under Art. 14, para. 2, items 1 – 3 APIA;
- the information provided more than three times according to the order of chapter three of the Civil Code;
- other information determined by law.

Managers are obliged to prepare an annual report on received applications for access to public information and for re-use of information from the public sector, which also includes data on the refusals made and the reasons for this. The annual report is part of the annual reports under Art. 62, para. 1 of the Law on

Administration (LA).[42]The information is published on the official websites of the administrations in the executive power system, created and declared as such on the basis of Art. 10, para. 3 EGA.[43]Other information is also published on the pages.[44]

Each manager is obliged to annually announce an updated list of the categories of information subject to publication on the Internet for the area of activity of the respective administration, as well as for the formats in which it is available.

The categories of information listed above under Art. 15 APIA are published, updated accordingly, within three working days from the adoption of the relevant act or from the creation of the relevant information, and if the act is promulgated - within three working days from the promulgation, unless otherwise specified by law term. The regulation of such a short term for publishing and updating the information is a guarantee of its relevance, which increases the control and accountability of the entities subject to the PDOI to the public.

APIA imputes an obligation to periodically publish up-to-date information not only on the heads of administrative structures in the executive power system, but also on two other groups of subjects obliged by law, namely:

- *public law entities, other than state bodies and local self-government bodies, including public law organizations*. They should periodically publish up-to-date information about their activities, corresponding to the information under Art. 15, para. 1, item 1, 4, 5, 6, 8, 11, 15, 16 and 17 APIA. The information is published on the websites of these entities;
- *organizations from the public sector, including public libraries, including and university libraries, archives and museums*. They should

[42]It is about the annual reports on the state of the administrations. The heads of administrative structures in the executive power system submit to the Secretary General of the Council of Ministers a report on the state of the respective administration annually by March 1.
[43]See Art. 10, para. 3 EGA- suppliers make public their official website.
[44]According to Art. 15, para. 2 DSOI in the "access to information" section of the websites of the administrations and public law entities, other than state bodies and local self-government bodies, including public law organizations, the data under Art. 15, para. 1, items 4 and 11 and the annual reports under para. 2, the existing internal rules regarding access to public information and the regulations for the costs of providing access to information under Art. 20, para. 2 GDPR and reuse of information from the public sector under Art. 41g APIA, the procedure for access to the public registers kept by the administrative structures in the executive power system.

publish all the conditions for providing the information for reuse on their website and on the portal under Art. 15 years APIA.

Along with the above, with amendments from 2015, several new provisions were created in APIA (Art. 15b - Art. 15d), which modernize the rules for access to public information, taking into account the technological progress of society and the new possibilities for searching and providing information , which information and communication technologies (ICT) provide.

Thus, Art. 15b APIA obliges every organization from the public sector to annually plan the step-by-step publication on the Internet in an open format of the information arrays and resources it maintains, access to which is free. The term "open format" is defined in § 1, item 8 AP of the GDPR as an electronic data format that does not require the use of a specific platform or specific software for the reuse of the content and is made available to the public without restrictions that would prevent the reuse use of information.

The publication of the planned information is included in the annual goals for the activity of the relevant administration under Art. 33a AL. At the proposal of the Minister of the Electronic Government at the Ministry of Electronic Government (MEU), the Council of Ministers annually adopts a list of data sets to be published in an open format on the Internet.

Art. 15c APIA regulates the creation and maintenance of a platform for access to public information - a single, central, public web-based information system that ensures access requests and publication of public information[45]. The administration of the Council of Ministers is obliged to create and maintain a platform for access to public information. The platform provides an opportunity to submit applications for access to information. State bodies, their territorial units and local self-government bodies, as obliged subjects under Art. 3, para. 1 of the Federal Data Protection Authority, publish on this platform the applications submitted through the platform, the decisions on them and the provided public information in compliance with the requirements for the protection of personal data

[45]§ 1, item 14 AP of APIA.

in relation to the applicant's data. In the case of refusal to grant access to public information, the decision is also served in accordance with the procedure of Art. 39 APIA by the relevant obliged entity.

Art. 15 of the ODAI, in turn, regulates the creation and maintenance of an open data portal – a single, central, public web-based information system that ensures the publication and management of information for re-use in an open, machine-readable format, together with relevant metadata.[46]The portal is built in a way that allows the complete retrieval of the published information or parts of it. This obligation is attributed to MEG. On this portal, public sector organizations publish the information under Art. 15b APIA (ie the information arrays and resources they support), access to which is free. The order and manner of publishing this information shall be determined by an ordinance adopted by the Council of Ministers.

The summary information about the bodies and their administrations in the volume prescribed by the FSA, as well as other information related to the implementation of the law, is included in the report on the state of the administration, which is adopted by the Council of Ministers. This information is published annually on a websiteof the Council of Ministers and the same must be available for citizens' reference in every administration.

It is noteworthy that the addressees of the obligations to publish public information prescribed by law are only the heads of administrative structures in the executive power system. Such a restriction is not justified - the heads of other state bodies and the bodies of local self-government and local administration remain outside the scope of the norm. The circle of persons should be expanded and the norm amended de lege ferenda.

5.4. Access to other public information

[46]§ 1, item 9 AP of APIA.

According to Art. 18 PDOI there are other cases of public information,which is relevant to society and the purposes of the law. This is information for the mass media, in particular information about:

- the persons who participate in the management of the relevant mass media or exercise effective control over the management or its activity;
- economically related persons who are involved in the management of other mass media, which allows them to exercise effective control over their management or their activities;
- the persons who are directly employed in the means of mass information and participate in the formation of the editorial policy;
- statements made about the public purposes of the mass information medium, as well as the principles or internal mechanisms that the mass information medium applies to ensure the credibility and objectivity of the information presented;
- the financial results of the media owner and the distribution of its output.

Access to this information is carried out in compliance with and balancing the principles of transparency and economic freedom, as well as the protection of personal data, trade secrets and the secrecy of the sources of mass information, who wished to remain anonymous.

5.5. Determining the costs of providing public information

In addition to being free, access to public information is also free. The costs of providing public information are paid according to the norms determined by the Minister of Finance, which cannot exceed the material costs of the provision. At the request of the applicant, information on the determination of these costs shall be submitted.[47]The additional costs for correcting or supplementing the provided public information are not paid in cases where it is inaccurate or incomplete and this is requested with a reasoned request by the applicant.

[47]Art. 20 APIA.

Obliged persons are obliged to announce the possible forms of providing access to public information at the place where the applications are submitted, the costs due and the methods of their payment.

The income from providing access to public information comes from the budget of the relevant authority.

6. Procedure for providing access to public information

Proceedings for access to public information are initiated on the basis of a written application or oral request.

The law expressly refers in art. 24, para. 2, that the application is considered to be in writing also in the cases when it is made electronically to the e-mail address of the relevant administrative structure (according to Art. 15, Para. 1, Item 4 APIA) or through the platform for access to public information according to Art. 15c APIA. In these cases, no signature is required, in accordance with the requirements of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and authentication services for electronic transactions in the internal market and repealing Directive 1999/ 93/EC (OB, L 257/73 of August 28, 2014) and of EDETSA. This provision specifies access to public information electronically, since in its old version, Art. 24, para. 2 FDSOI requires each body to determine the procedure for providing access to public informationelectronically. This rule raises a number of questions and uncertainties[48], especially in the light of the relationship between EDETSA, EGA, as newer laws on the one hand, and APIA, as an older law - on the other hand. With the new edition of the provision, it is now clearly indicated that the application for access to public information, submitted electronically, does not need to be signed with an electronic signature (a qualified electronic signature is meant - author's note). This lightening of the form should be evaluated positively. It can be explained by the importance of access to public information for accountability and control over the activities of the obliged entities.

[48]See Dimitrov, G. Right to information and communication technologies. Part II. Administrative legal and technological aspects, Electronic management. Legal regime of information. Legal Regime of Cryptography. Standardization in the field of ICT. Sofia, Law and Internet Foundation, 2014, chapter III, section 3.6.

It is important to note that in order to facilitate access to public information, APIA imputes to the obliged entities the obligation to provide access even upon verbal request. The light form is justified, in view of the important function of access to public information. When the applicant did not get access to the requested information based on an oral inquiry or considers the information provided to him to be insufficient, he may submit a written application.

The application for granting access to public informationmust contain the details specified in the law.[49]Applications are subject to mandatory registration in accordance with the procedure determined by the relevant authority.

As far as the forms (ways) of providing access to public informationare different and – to make it clear that they are all available to subjects – the law states that they can be:

- review of the information - original or copy, or through a publicly accessible register;
- oral reference;
- physical media copies;
- copies provided electronically or at the Internet address where the data is stored or published.

It is up to the subject what form he chooses. Moreover, these forms are not alternative - they can be used in combination or separately.[50]When the preferred form of providing access to public informationis the provision of the data electronically or at an Internet address where the data is stored or published, the technical parameters for recording the information are also determined. Persons with visual or auditory-speech impairments may request access in a form appropriate to their communication capabilities.

[49]Art. 25, para. 1 APIA. In addition, the indication of the purpose for which access to public information is requested, is an essential and mandatory condition when submitting an application for access to information. Decision No. 4962 of April 8, 2011 of the Supreme Administrative Court under Adm. e. No. 9086/2010
[50]Art. 26, para. 2 APIA.

It is important to pay attention to the fact that the law obliges authorities to comply with the preferred form of providing access to public information, except in cases where:

- there is no technical possibility for it;
- it is related to an unreasonable increase in the costs of providing it;
- leads to the possibility of illegal processing of this information or copyright infringement.

In these cases, access to the information is provided in a form determined by the authority.

Applications for providing access to public informationare considered in the shortest possible time, but no later than 14 days after the date of registration of the application. The term for providing access may be extended, depending on the volume and technological time for providing the information, but by no more than 10 days. In all cases, the postponement must be motivated.

The term can be extended by up to 14 days in cases where the requested public information refers to a third party and his consent is required for its provision. In these cases, the authority is obliged to request the express written consent of the third party within 7 days of registering the application and to strictly observe the conditions under which the third party has given consent to provide the information concerning him. In case of express disagreement by the third party within the period under para. 1 APIA, the relevant authority provides the requested public information in a volume and in a way that does not reveal the information affecting the interests of the third party.

The authorities decide to grant or refuse to grant access to the requested public information and notify the applicant in writing of their decision.

In the event that the will of the applicant does not make it clear exactly what information he wants, he is notified of this by the authority and is given the right to specify the subject of the requested public information. In these cases, the deadline for providing begins to run from the date of specifying the subject of the requested

public information. If clarification does not follow within 30 days, the application is left without consideration.

When the authority provides access to the requested public information, it must state in its decision:

- the extent of the provided access to the requested public information;
- the period in which access is provided;
- the location where access will be provided;
- the form in which access will be provided;
- the costs of providing access.

The decision may indicate to the applicant which other authorities, organizations or persons have more complete information.

The decision to grant access to the requested public information is delivered to the applicant against a signature or sent by mail with return receipt, or sent electronically when the applicant has requested that the information be provided to him electronically and has specified an e-mail address .

Access to public information is granted after payment of the specified costs and presentation of a payment document. It should be borne in mind that the obligation to pay the costs of the body providing the public information has a quasi-public law nature, but is not an obligation to pay a fee. This is a special type of obligation that arises in favor of the entities obligated under this law – authorities, public law organizations and individuals, private individuals and legal entities. Its size cannot be initially determined, due to the different nature of the public information to which access is requested, as well as the ways (forms) of providing it.

For providing access to public informationa protocol is drawn up, which is signed by the applicant and the relevant employee. When the applicant has requested that access to information be provided electronically and has specified an e-mail address for receipt, the authority sends to the specified e-mail address the decision on granting access together with a copy of the information or the Internet address where it is contained the data. In these cases, a protocol is not drawn up

and no provision costs are paid. In this sense, the request to obtain access to public information in the form of copies provided electronically or at the Internet address where the data is stored or published emerges as a fast, cheap and convenient alternative for individuals and their entities .

If the applicant has changed the e-mail address without notifying the authority, or has indicated an incorrect or non-existent address, the information is considered received from the date it is sent. This permission is justified, because the entities obliged under the Personal Data Protection Act have no way to check the actuality and correctness of the address specified by the applicant - this is legally considered a burden on the applicant.

If the applicant does not appear within the specified period or when he does not pay the specified costs, it is assumed that the applicant has lost interest in the access granted to him to the requested public information. This rule does not apply when the application is submitted through the public information access platform or electronically.

As indicated above, providing access to public informationmay be refused in cases specified by law. In such scenarios, if access can only be granted to certain information, access to which is not restricted, then partial access is granted.

In the decision to refuse to provide access to public informationthe legal and factual grounds for refusal, the date of acceptance of the decision and the order for its appeal shall be indicated.[51]It is handed to the applicant against a signature or sent by post with return receipt. These decisions are subject to appeal before the relevant administrative court in accordance with the law.[52]There is a legal imperative for a written ruling on the application, including in case of refusal.[53]This requirement automatically raises the question of the regime of tacit refusal to grant access to public information.[54]It has been established that a silent

[51]Art. 38 APIA.
[52]Art. 40 et seq.
[53]Decision No. 8512 of June 13, 2012 under Adm. e. No. 9701/2011 of the Supreme Court.
[54]This is so because the court binds the requirements under Art. 34 PDOI, referring to the decision to grant access to public informationwith the decision to refuse to provide one. Thus, according to Art. 34 APIA, the decision to provide access to public information, respectively the refusal to provide such, should be prepared in writing and

refusal under the GDPR is not equivalent to a decision to refuse to grant access to the requested information.[55]

7. Control

Failure to fulfill the obligation to provide access to public information is an administrative violation, unless the failure itself constitutes a crime.

If a violation is established, the relevant official shall be subject to an administrative sanction - a fine in the amounts established by law.[56]The establishment of the violation is carried out by the relevant authority, when it was carried out by an official working in the administration of a state body, in its territorial unit or in a local self-government body. When the perpetrator is an official working in an administration, a public legal entity or an organization other than the specified authorities, or is a natural or legal person carrying out an activity financed with funds from the consolidated state budget and with funds from European Union funds, or provided by the European union on projects and programs, the establishment of the violation is carried out by officials appointed by the Minister of Justice. Violations of the requirement that public sector organizations publish in an open format the information arrays and resources they maintain on the open data portal maintained by MEG and provide free access to this information are established by officials authorized by the MEG chairman .

Penalties are drawn up for the committed violations.

Violations are established, and penalties are imposed, appealed and executed in accordance with the Law on Administrative Violations and Penalties.

---

have the content prescribed by law. Given the imperativeness of this requirement of the law, the tacit refusal to provide access to public information contradicts the above provision and was correctly accepted by the deciding court as a violation of the requirement for the content of the individual administrative act, which was considered a particularly significant procedural violation and grounds for annulment of the contested act. Decision No. 2470 of February 20, 2013 under Adm. d. No. 4596/2012 of the Supreme Court.

[55]Due to this fact, the rule of Art. 173, para. 2 APC, not that under Art. 41, para. 1 APIA. Decision No. 13947 of November 19, 2010 of the Supreme Administrative Court under Adm. e. No. 2357/2010

[56]Art. 42 APIA.

8. Trends in the development of the EU framework of access to public information and its impact on the Bulgarian legislation

The research shows that two main trends in the development of the EU regulatory framework regarding access to public information are at place, which could influence the Bulgarian legislation.

8.1. Streamlining reporting obligations

In recent years, a key trend in the EU has been the streamlining of reporting obligations across various directives and regulations, particularly in the context of public information access. This trend reflects the EU's commitment to simplifying administrative processes and reducing redundancies in the legislative framework, thereby enhancing efficiency and coherence across Member States.

One of the main objectives of streamlining reporting obligations is to eliminate overlapping requirements that often result in unnecessary administrative burdens on public authorities and organizations. Multiple EU directives, especially in fields like environmental protection, can have intersecting reporting requirements. By consolidating these obligations, the EU aims to facilitate a more integrated and straightforward reporting process. This not only saves time and resources but also improves compliance rates and the quality of reported information.

Moreover, this trend aligns with the EU's broader strategy of digitalization and modernization of public administration. Implementing unified and streamlined reporting mechanisms often involves leveraging digital technologies, which can automate data collection and processing, enhance data accuracy, and ensure timely access to information for both authorities and the public.

In summary, streamlining reporting obligations in the EU represents a pragmatic approach towards regulatory efficiency. It balances the need for comprehensive oversight with the practicalities of administrative workload, thereby fostering a more effective and user-friendly regulatory environment. This

trend is crucial for supporting the EU's vision of a transparent, accountable, and responsive governance structure.

8.2. Transparency in EU trade negotiations – a forward thinking approach

The EU has recently emphasized enhancing transparency in trade negotiations, a trend that marks a significant shift in its approach to international trade agreements. This focus on transparency was notably exemplified in the negotiations for the Transatlantic Trade and Investment Partnership (TTIP). The EU's strategy in the TTIP negotiations represents a move from traditional closed-door negotiations to a more open and inclusive process, intending to build trust and support from the public and stakeholders.[57]

This new approach involves providing broader access to negotiation documents and more comprehensive information about the negotiation processes. The EU aims to make the information not just accessible but also comprehensible to the public, ensuring that stakeholders and citizens can engage more meaningfully with the contents and implications of trade agreements. This paradigm shift underscores the EU's recognition of the importance of public opinion and the need for democratic legitimacy in trade policies.

The transparency strategy in trade negotiations also reflects the EU's commitment to accountability. By making negotiation processes more visible, the EU opens itself to scrutiny and feedback, which can lead to more balanced and equitable trade agreements. This approach is expected to serve as a model for future trade negotiations, setting a precedent for transparency and public participation as integral components of international trade policy.

Overall, this trend towards transparency in trade negotiations demonstrates the EU's progressive stance in adapting its policies to contemporary expectations of openness and public engagement in policymaking. It aligns with broader global

[57] Marx, A., & Loo, G. (2021). Shape of Transparency in EU Trade Policy: A Focus on Free Trade Agreements. Politics and Governance, 9 (1) (https://dx.doi.org/10.17645/PAG.V9I1.3771 https://www.cogitatiopress.com/politicsandgovernance/article/view/3771).

trends towards greater transparency in governance and can contribute to more sustainable and publicly supported trade policies.

III. REUSE OF PUBLIC SECTOR INFORMATION

1. Concept of information from the public sector. Difference between public sector information and public information

The concept of "public information" should be distinguished from the concept of "public sector information". As it became clear from Module 2, public information is that which is contained in the acts of state bodies and local self-government bodies in the exercise of their powers and that which is collected, created and stored in connection with official information, as well as reason for the activities of the bodies and their administrations.

The scope of the concept of "public sector information" ismuch wider.

This is any information objectified on a tangible medium, including stored as a document, and collected or created by a public sector organization.

Material medium is any paper, technical, magnetic, electronic or other medium, regardless of the type of recorded content – text, plan, map, photograph, audio, visual or audio-visual image, file and the like.

According to APIA, information from the public sector is also maintained in electronic form. It may not be contained in the acts of state bodies and local self-government bodies, nor was it collected, created or stored in connection with official information or on the occasion of the activities of the bodies and their administrations, but in any case it covers public information , regardless of its type.

The range of addressees of the obligation to provide information is also different. As it became clear, persons obliged to provide access to public informationare the state bodies, their territorial units and local self-government bodies, as well as public law entities, outside of these, including public law organizations. Obliged to provide access to public information include individuals and legal entities regarding their activities, financed with funds from the consolidated state budget and with funds from European Union funds or provided

by the European Union under projects and programs. The circle of persons obliged to provide information from the public sector for re-use is much narrower. These are only public sector organizations - state bodies, local self-government bodies, public law entities other than these bodies, including public law organizations.

Establishing a wider scope of persons obliged to provide access to public informationis understandable. Society's interests in publicity and transparency require the possibility of access to information stored in a larger group of persons.

The rationale behind the provision of a right to reuse public sector information rests on the concept that all information collected by public sector organizations should be freely usable by all interested parties for commercial or non-commercial purposes other than the original purpose, for which it was created. Its use can help to make more efficient use of investment in the creation of certain information in the public sector and contribute to the fuller realization of the economic potential of this information, with a view to providing value-added services and increasing competitiveness.

For example, a person has the right to take the meteorological data collected by the National Institute of Meteorology and Hydrology and use it to create a fully commercial service – for example, a weather forecast application for a mobile phone. How the information is used is entirely up to the person concerned.

Attention should be drawn to the fact that the provision of public sector information to a public sector organization in connection with the exercise of its powers or functions is not reuse within the meaning of this Act.

The main principles in providing information from the public sector for re-use are:

- ensuring the possibility of multiple reuse of information from the public sector;
- transparency in providing information from the public sector;
- prohibition of discrimination in the provision of information by the public sector;
- prohibition of restriction of free competition.

All rules affecting access to public information regarding the limits of the right to provide information, the circle of persons who have the right to request its provision, and the permissible limitations of the right of access, apply accordingly to the right to reuse information from the public sector.

2. Procedure for reuse of information from the public sector

The prerequisites for providing information from the public sector aboutreuse are separated into several groups.

Public sector information is provided in the format and language in which it was collected, created, or otherwise. Although the interested party can indicate their preferences, the discretion is left to the public sector organisation. It is also possible to provide the information in an open, machine-readable format, together with relevant metadata. The provision of the data in an open machine-readable format is carried out in accordance with the objectives under Art. 15b APIA, i.e. in accordance with the objectives related to ensuring the gradual publication on the Internet of the information arrays and resources that the relevant organization from the public sector maintains and to which access is free. The format and metadata in these cases conform to official open standards.

An obligation for public sector organizations to provide information for re-use does not arise where this requires its creation or adaptation, or where it involves the provision of parts of documents or other material which requires a disproportionate amount of effort beyond the scope of a normal operation . The purpose of this rule is to provide the information "as is". The public sector organization cannot be expected to process the information outside of the way it is carried out within the framework of its normal work. Any other processing is left to the discretion and responsibility of the interested party when they receive the information.

Public sector organizations are not obliged to continue the creation or collection of a certain type of information for the needs of its reuse when, within

the framework of the operational independence of the public sector organization, it is judged that it will no longer be collected and processed. The organization is obliged to satisfy the right of the interested person to receive only information available from the public sector or such that the organization creates within the framework of its normal, usual work in the exercise of its powers.

At the request of the applicant and if possible, the requested information is provided electronically to the email address or by other appropriate means of providing the information in electronic form.

With a by-law - the Ordinance on the standard conditions for the reuse of information from the public sector and for its publication in an open format, adopted by the Council of Ministers on the basis of Art. 15d, para. 3 PDOI – standard conditions are defined for the reuse of information from the public sector and for the publication of information from the public sector in an open format for commercial or non-commercial purposes. The EPA stipulates that these conditions may not impose unnecessary restrictions on re-use opportunities or restrict competition. The logic of this rule is that the conditions introduced for providing access to such information do not create unnecessary obstacles from an administrative or competition law point of view to the reuse of information by the public sector. Its re-use should not be restricted by unnecessary administrative formalities and encourage entrepreneurship and free competition in the market.

The public sector organizations provide the information for re-use unconditionally or under the conditions determined by them within the standard conditions defined in the Ordinance on the standard conditions for the re-use of information from the public sector and for its publication in an open format.

APIA also introduces a special rule regarding the provision for re-use of information representing an object of intellectual property and for which libraries, including libraries of higher education institutions, museums and archives, have the right to use. Such information is provided for re-use if such re-use is permitted by the relevant rights holder. This permission is justified - only the holder of the relevant intellectual property right can permit or prohibit such use of the

information, and this circumstance has also been taken into account by the legislator.

The reuse of information from archives - documents from the National Archives Fund - is carried out under the conditions and according to the order of chapter six of the National Archives and in compliance with this law.

Public sector information may not be made available for reuse:

- the content of which is related to an activity falling outside the powers and functions of the organizations from the public sector, according to law, organizational act or statute, and/or an act by which the public task was assigned;
- which is the subject of a third party's intellectual property right;
- which is collected or created by public broadcasters or their regional centres;
- property of schools, higher education institutions (except for libraries of higher education institutions), scientific and research organizations, including organizations established for the dissemination of results of scientific research activities, and of cultural organizations, with the exception of libraries, museums and archives;
- constituting classified information;
- containing statistical secrets collected and stored by the National Statistical Institute or by a statistical authority;
- containing a production or trade secret or a professional secret within the meaning of the law;
- for the receipt of which the applicant must prove a legal interest, according to law;
- representing parts of documents that contain only emblems, coats of arms and insignia;
- containing personal data, the reuse of which constitutes impermissible access or impermissible processing of personal data, according to the requirements for their protection.

In the above cases, only that part of the information to which access is not restricted is provided for reuse.

However, in cases of overriding public interest, the public sector organization is obliged to provide for re-use information containing a production or commercial secret. The logic is that, in this case, the interests of society prevail over the private interest of the organization concerned, and it cannot refuse to provide the requested information, citing its own production and trade secrets. APIA nevertheless contains certain guarantees protecting the interests of the public sector organization, which must disclose its production and trade secrets on the basis of an overriding public interest. In the event of such disclosure, the public sector organization may prohibit re-use for commercial purposes or in a manner that would result in unfair competition or other restriction of competition within the meaning of Title Two of the Competition Act.

Information from the public sector is provided for re-use also to organizations from the public sector under the conditions and in accordance with the law. As a rule, one public sector organization cannot pay fees to another. However, if public sector information is requested for re-use by another such organization in connection with carrying out activities that are outside its powers or functions, the same conditions and payment apply as for all interested parties.

The search for information from the public sector should be facilitated by the organizations providing it. They should provide for this by maintaining and publishing lists of core documents and relevant metadata through various online access mechanisms and in machine-readable format or by other appropriate means, for example through specialized applications. Where possible, public sector organizations provide conditions for multilingual search of documents.

The provision of information by the public sector cannot be restricted by contractual clauses. The conclusion of contracts for the exclusive provision of information by the public sector is prohibited. Thus, the other interested parties would be deprived of the benefit of benefiting from the information collected or collected at the expense of a market agent. This is unacceptable and the law prohibits it. There can be an exception only in two cases:

- when the provision of a service of public interest cannot be ensured in any other way. The existence of grounds for concluding such a contract

is reviewed every three years by the public sector organization that is a party to it;

- where the granting of an exclusive right of re-use is related to the digitization of cultural resources, in which case the term of validity shall not exceed 10 years, and if it exceptionally exceeds 10 years, the term of the contract shall be reviewed on the eleventh year after its entry into force, and every next 7 years. The provisions of this contract relating to the granting of exclusive rights shall be made public. Public sector organizations provide data on the manner and criteria by which the contractor under this contract was determined. The contract must include the right of the public sector organization to receive a free copy of the digitized cultural resources. After termination of the exclusive rights under the contract, this copy is made available for reuse.

3. Procedure for providing information from the public sector for re-use

The exercise of the right to provide information by the public sectorfor reuse begins at the initiative of the interested party, based on a written request. The request is also considered to be in writing in cases where it is made electronically to the e-mail address of the public sector organization or to the open data portal created and maintained by MEG.

When the request is submitted electronically, public sector organizations are required to respond electronically as well. In this case, confirmation of receipt of the response is not required. This norm is generally unnecessary because according to the Law on e-Governmentall public sector organizations fall under its addressees and they are obliged to provide all their services electronically[58], in particular the provision of information by the public sector. The provision of public sector information for re-use by electronic means qualifies as an electronic administrative service and is subject to all provisions of the WEU.[59]

[58]See Art. 8, para. 2 EGA.
[59]See Art. 8, para. 1 in connection with §1, item 2 AP to EGA.

Public sector information is provided for reuse free of charge or upon payment of a fee that cannot exceed the material costs of reproducing and providing the information.

The stated principle for determining the fee does not apply to fees collected:

- from organizations from the public sector, which, by virtue of the act of awarding the public task, are obliged to generate income to cover a significant part of the costs related to the performance of the public task; the obligation to realize revenues is determined in advance and published electronically;
- for the re-use of information in respect of which the public sector organization is obliged to realize sufficient revenue in order to cover a significant part of the costs related to the collection, production, reproduction and dissemination of the information, according to law or established administrative practice; the obligation is determined in advance and published electronically;
- from libraries, including university libraries, museums and archives.

In the first two cases, the public sector organization calculates the total fees depending on the categories and amount of data provided for reuse, in accordance with objective, transparent and verifiable criteria determined by a methodology adopted by the Council of Ministers. The public organization's total revenue from supplying and allowing the reuse of the information for the relevant accounting period must not exceed the costs of collection, production, reproduction and distribution, together with a reasonable return on investment, calculated in accordance with the accounting principles applicable to the public organization.

The logic of the law is that this payment must be cost-oriented. The provision of public sector information should not become a source of profit for the public sector organisation. It collects information within the powers granted to it by law. Therefore, the organization's budget covers the cost of acquiring, creating and maintaining it. From there, the cost should be determined only by the additional time and material resources necessary to prepare and provide it on demand, which includes human time, resources for the creation of physical copies, courier costs, etc.

In cases of provision of information by libraries, including libraries of higher education institutions, museums and archives, the total income from the supply and permission to reuse the information for the relevant accounting period must not exceed the costs of collection, production, reproduction, distribution, storage and the acquisition of rights to use the information, together with a reasonable return on investment, calculated in accordance with the accounting principles applicable to the public organization.

The amount of fees is determined:

- for fees collected by a state body - with a tariff adopted by the Council of Ministers;
- for the fees collected by another organization from the public sector - by the head of the organization;
- for the fees collected by the municipalities - by the municipal council, and the fees determined may not exceed the fees determined by the tariff of the Council of Ministers.

The amount of fees, the basis on which they are calculated, the factors taken into account in the calculation, as well as any additional conditions, if any, are published, including electronically in the presence of a website. Upon request, the manner in which these fees were calculated in relation to the specific reuse request shall also be specified. The amounts of fees for re-use of information go to the budget of the relevant organization from the public sector. The Council of Ministers reviews every three years the methodology for determining the fees based on a summary report on the availability of reuse information provided by public sector organizations, the conditions under which it is provided and legal protection practices prepared by MEG on every three years.

If a public sector organization that is not a government body does not set fees in accordance with the above principles, the organization provides this information for reuse free of charge or upon payment of a fee determined by the Council of Ministers tariff.

The request to provide information from the public sector for re-use is considered within 14 days from his entry. In many cases where the requested information is relevant over a period of time, public sector organizations must provide it within a reasonable time frame in which the information has not lost its relevance.

In the studied case - the provision of data on meteorological measurements, the information must be provided immediately or within a few hours. Otherwise, the applicant will lose legal and economic interest in receiving it.

However, when the request for reuse of public sector information is characterized by complexity and requires more time to provide it, the deadline can be extended by another 14 days.

For example, where a public sector organization has a branch structure and registers that are kept by hand, the collection of information relating to the registers – number of entries, types of entries, etc. – could not be provided within 14 days, because the logistics of collecting and providing this data requires technological time. In this case, the applicant is sent a message about the time required to provide the information within 14 days of receiving the request.

If there is a reason to refuse to provide public sector information for re-use, the public sector organization must give reasons for the reasons. Such reasons can only be a legal prohibition to provide the requested information (for example, it constitutes classified information) or the request does not formally meet the requirements of the law (for example, the request is not made in writing).[60]The refusal must clearly contain the factual and legal basis for the refusal, the date of the decision and the procedure for appealing it. In case of refusal due to the existence of intellectual property rights belonging to a third party, the refusal decision shall indicate the name of the holder of the rights (natural or legal person) or the person from whom the public sector organization received the information and the permission to use it. Libraries, including university libraries, museums and archives, are not required to identify these individuals. It is important to note that

[60]Art. 41 is APIA.

in many cases the requested information contains personal data about certain individuals. As a rule, providing such information for reuse is prohibited. It is permissible only when the availability of personal data constitutes or is part of a publicly accessible register - for example, the commercial register and register of non-profit legal entities, BULSTAT register, etc.

In order to increase accountability regarding the reuse of information from the public sector, MEG is scheduled to prepare every three years a summary report on the availability of information for reuse provided by public sector organizations, the conditions under which it is provided, and the practices for Legal protection. Organizations from the public sector annually send reports on these circumstances to the administration of the Council of Ministers. The report shall be made public and provided to the European Commission.

4. Trends in the development of the EU framework of reuse of public information and its impact on the Bulgarian legislation

The research shows several trends in the development of the EU policies with respect to reuse of public information. These should be considered since they could influence the development of the Bulgarian legislation in the near future.

4.1. Expansion of Directive scope

The possibility of including public research and educational establishments in the Directive regulating the reuse of public sector information is a significant trend.[61] This expansion would broaden the scope of the Directive, which currently focuses on governmental data, to encompass a vast array of research and educational data.

This inclusion could have profound legal consequences, potentially transforming how research and educational data are accessed and reused. It raises

[61] Richter, H. (2018). Including Public Research and Educational Establishments within the Scope of the Directive regulating the re-use of public sector information ('PSI Directive') (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090337).

questions about the balance between open access to information and the protection of intellectual property rights, especially in research-intensive fields.

The trend reflects a growing recognition of the value of educational and research data in driving innovation and economic growth, as well as the need for clear legal frameworks to govern their reuse.

4.2. Economic focus in policy development

The development of the EU regulatory framework for public sector data is increasingly skewed towards economic considerations. This trend indicates a shift from viewing public sector information merely as a governmental resource to seeing it as a key economic asset.[62]

This economic prioritization sometimes overshadows concerns about fundamental rights and democratic values. It raises critical questions about data privacy, citizen rights, and the ethical use of public sector information.

The trend underscores the EU's intent to leverage public sector data as a driver of economic growth, particularly in the digital economy, but it also calls for a balanced approach that respects democratic values and individual rights.

4.3. Consideration of national contexts

Policies on the reuse of public sector information in the EU increasingly recognize the importance of national contexts.[63] This trend acknowledges that a one-size-fits-all approach may not be effective across diverse national settings.

The impact of these policies on organizational structures and economic prosperity varies significantly from one country to another, influenced by each nation's unique public sector landscape, legal framework, and economic conditions.

---

[62] Buttow, C. V., & Weerts, S. (2022). The development of the European Union regulatory framework governing the availability, sharing, and reuse of public sector data (https://journals.sagepub.com/doi/10.1177/20539517221124587).

[63] Koerten, H., & Veenswijk, M. (2013). Organizational Consequences of Policies on the Reuse of Public Sector Information in Europe (https://content.iospress.com/articles/journal-of-e-governance/gov00356).

This trend suggests a move towards more tailored policies that respect and adapt to national differences, aiming to maximize the economic and innovative potential of public sector information reuse within each unique national setting.

4.4. Competition law and PSI reuse

The interplay between competition law and the regulation of PSI reuse is a growing trend in the EU.[64] This focuses on how the principles of competition law apply to entities reusing public sector information.

Key issues include the definition of 'undertaking' in the context of PSI and the implications for public sector bodies that engage in economic activities. This trend is crucial in determining the extent to which public sector bodies are subject to competition rule.

This trend reflects the EU's effort to ensure fair competition in the digital marketplace, particularly where public and private entities converge, and highlights the need for clarity in legal interpretations to foster a competitive and fair environment for PSI reuse.

4.5. Legal regulation and access to PSI

The legal regulation of access to public sector information in EU countries is increasingly shaped by EU-wide legal frameworks. The focus is on setting minimum rules for transparency, preventing discrimination, and ensuring fair trade practices in the reuse of PSI.[65]

Despite these efforts, the full potential of public sector information is not fully realized, often hindered by barriers such as fees for access. This trend points to ongoing challenges in balancing public access with revenue models for PSI.

The trend highlights the EU's commitment to making public sector information more accessible and usable, but it also underscores the need for

[64] Drexl, J. (2014). The European Framework for the Regulation of PSI in Terms of Competition (https://china.elgaronline.com/edcollchap/edcoll/9781784714970/9781784714970.00013.xml).

[65] Janssen, K. Legal Regulation of Access to Public Sector Information (https://link.springer.com/chapter/10.1007/978-3-030-23665-6_27).

continued efforts to remove barriers and to fully harness the potential of PSI for societal and economic benefits.

IV. CLASSIFIED INFORMATION

1. Concept of classified information

Special legal protection by the laws is given to the so-called "classified information". The creation, processing, storage, conditions and procedure for providing access to it are governed by a special Law on the Protection of Classified Information)[66]and are detailed in the Regulations for its implementation.[67]

Classified information within the meaning of the law is information representing a state or official secret, as well as foreign classified information provided by another country or by an international organization, insofar as an international treaty in force to which the Republic of Bulgaria is a party does not provide otherwise.

Classified information is a legally protected secret, access to which is strictly limited.[68]It is granted only to persons who have been granted access permission when their official duties or a specifically assigned task require such access, and only to certain classified information.[69]

2. Bodies for the protection of classified information

2.1. State Commission on Information Security

The state body that implements the policy for the protection of classified informationinformation in the country is the State Commission for Information Security (SCIS). It is a collective body and consists ofof five members, including a

[66]Pron. SG. no. 45 of April 30, 2002, final change SG. No. 17 of February 26, 2019
[67]Adopted by PMS No. 276 of 02.12.2002. Pron. SG. no. 115 of December 10, 2002, final change and add. SG. no. 68 of 22 August 2017
[68]See Pavlov, G. Problems of security and protection of classified information in automated information systems and networks. // Economic Alternatives, UNSS, "National and Regional Security" Department, no. 5/2005. URL: <http://alternativi.unwe.bg/alternativi/index.php?nid=5&hid=72> (24.10.2019).
[69]The so-called "need to know" principle - Art. 3, para. 2 PPE.

chairman and a deputy chairman, who are determined by a decision of the Council of Ministers for a term of 5 years on the proposal of the Prime Minister. SCIS is assisted by an administration whose activity, structure and organization of work are determined by organizational regulations adopted by the Council of Ministers.[70]

DSKI organizes, implements, coordinates and supervises the activity on the protection of classified information and ensures equal protection of classified information. The Commission carries out its activities in close cooperation with the bodies of the Ministry of Defence, the Ministry of Internal Affairs, the Ministry of Foreign Affairs and the security and public order services.

In order to carry out its activities, the SCISM has precisely defined powers in the field of classified information in the law - the most important of which can be summarized as follows: the SCISM (1) defines guidelines for working with such information and action plans in the event of various incidents, related to its disclosure; (2) performs an analysis and assessment of readiness for the protection of classified information in various incidents related to unregulated access to classified information, and gives mandatory instructions in this area; (3) conducts preventive activities; (4) prepares and proposes drafts of normative acts to the Council of Ministers; (5) organizes the activity of registries in international relations; (6) organizes, supervises and is responsible for the fulfillment of the obligations for the protection of classified information contained in international treaties to which the Republic of Bulgaria is a party; (7) carries out guidance on reliability studies of persons who need to work with classified information, and on the issuance of permits to persons to work with classified information, as well as on the issuance of certificates for persons working under various contracts in this district; (8) carries out research and issues decisions on the appointment of information security officers and makes decisions on the issue or refusal of a permit to work with classified information to persons who have been identified as belonging to the State Security and Intelligence Services of the Bulgarian People's Army[71]; (9) issues certificates confirming to foreign authorities that Bulgarian

[70]Rules of Procedure of the State Commission on Information Security and its Administration, adopted by PMS No. 38 of 22.02.2017, promulgated, SG No. 19 of 28.02.2017, in force from 28.02.2017 in force from 28.02.2017
[71]See Art. 9, item 9a cf. art. 45a, paragraph 3 of the Civil Code.

individuals or legal entities possess a permit, corresponding certificate; (10) keeps the registers provided for in the law for issuing permits; (11) organizes training in the field of classified information; (12) carries out general control over the protection of classified information created, stored, processed and transmitted in communication and information systems; (13) carries out reception, storage, transfer and delivery of documents and/or materials containing classified information, etc.[72]

2.2. Security services

Security services are created under various departmentsfor the purpose of conducting reliability studies of its employees and job applicants with classified information.

According to the law, security services are the State Intelligence Agency, the National Security Service, the State Agency for National Security (DANS), the Main Directorate for Combating Organized Crime and the Directorate for Internal Security of the Ministry of Internal Affairs, the Military Information Service of The Ministry of Defence, the State Agency "Technical Operations" and the following bodies of the Commission for Combating Corruption and Confiscation of Illegally Acquired Property (KPCONPI) - the director of the Directorate, which carries out anti-corruption activities by collecting, analyzing and checking information at and on the occasion of information about acts of corruption of persons holding high public positions, as well as the inspectors therein.

Security services issue, terminate and revoke the clearances of their employees and applicants for work with classified information. With respect to individuals and legal entities that apply to conclude or that execute a contract related to access to classified information, they carry out the necessary studies and issue certificates of compliance with security requirements, according to the law.

The security services assist the SCIS in the exercise of its powers and cooperate with each other.

[72]See Art. 9 PPE.

The security services in the Ministry of Defence, the structures directly subordinated to the Minister of Defense and the Bulgarian Army, with the exception of the "Military Information" service, also have the functions of conducting studies, issuing, terminating and revoking permits of Bulgarian citizens - military personnel in military service, from the reserve and civilian employees in an official or employment relationship in the Ministry of Defense, the structures directly subordinated to the Minister of Defense and the Bulgarian Army; carrying out studies, issuing, terminating and revoking permits of natural persons, respectively certificates of legal entities applying for or carrying out activities for the needs of the Ministry of Defense, the structures directly subordinated to the Minister of Defense and the Bulgarian Army and issuing confirmations to foreign citizens for work and/or training in the Ministry of Defense, the structures directly subordinated to the Minister of Defense and the Bulgarian Army.

All security services have the right to apply and use intelligence methods under conditions and in accordance with the law; to apply and use special intelligence means, under the conditions and in accordance with the Law on Special Intelligence Means (SIR), for persons applying for permission to access information with a security classification level of "Top Secret"; to use, process and store data on individuals and legal entities - the subject of research, data on cases of unregulated access to classified information, etc. They have the right to receive the necessary information from state authorities, local self-government bodies, natural and legal persons, according to the laws in force. The conditions and procedure for providing the information are in accordance with the procedure established in the regulations for the implementation of the law.

Officials designated by the chairman of the National Security Agency carry out direct control over the protection of classified information and compliance with legal provisions, having the right of access to objects and premises; access to documents related to the protection of classified information; access tokcommunication and information systems, including those connected to theminformation systems, in order to establish reliability and their protection; to demand explanations from managers and employees; to bring in experts when special knowledge is needed to clarify circumstances in connection with an

investigation being carried out and to give prescriptions in relation to the protection of classified information. The procedure for carrying out inspections is determined by the Ordinance on the procedure for carrying out inspections for the implementation of direct control for the protection of classified information (NRIPOPKZKI)[73].

DANS is a security service with special competences.

Outside of the general functions of a security service, it performs reliability investigations of persons required to work with classified information and issues, terminates, revokes or denies access to the appropriate classification level; issues confirmation to foreign individuals or legal entities on the basis of a permit or certificate already issued by the relevant competent authority of another country or international organization and after an investigation has been carried out in the Republic of Bulgaria, and carries out direct control over the protection of classified information and compliance with legal provisions in this area.

In addition, DANS is also charged with the functions of carrying out activities on the cryptographic protection of classified information, according to the Law on the State Agency "National Security"[74]. It issues, revokes and terminates certificates (certificates) for the security of communication and information systems, coordinates and controls TEMPEST countermeasures[75]and carries out and supervises the training for working with cryptographic methods and means of the persons granted permission to access classified information.

[73]In force since February 28, 2003, adopted by PMS No. 44 of February 21, 2003; Pron. SG. No. 19 of February 28, 2003, amended. SG. no. 44 of May 9, 2008

[74]Pron. SG. No. 109 of December 20, 2007, final change and add. SG. No. 17 of February 26, 2019

[75]§ 1. item 25 of the AP of ZZKI defines "TEMPEST" as research, study and control of compromising electromagnetic radiation and countermeasures for their suppression and limitation, and item 26. defines "TEMPEST countermeasures" as security measures intended for purpose of protection against unregulated access to classified information through compromising electromagnetic radiation.

2.3. Public order services

Law enforcement agencies are investigatingfor the reliability of their employees and job applicants, issue, terminate and revoke the permits of these persons.

The public order services are the Main Directorate "National Police", the Main Directorate "Border Police", the Main Directorate "Fire Safety and Protection of the Population" and the regional directorates of the Ministry of Internal Affairs, the "Military Police" service under the Minister of Defense.

When carrying out their activities, the public order services have the right to apply and use operative-search methods and means under conditions and according to the law; to use, store and process data from their databases for individuals and legal entities - the subject of research; to store the data obtained in the process of surveying their employees; to store data on cases of unregulated access to classified information and to receive any necessary information from other organizational units in connection with the investigations of persons working with classified information.

The public order services, within the limits of their functions and powers, are obliged to provide assistance to the security services in connection with the performance of the tasks of the security services.

2.4. Organizational units

Organizational units are all bodies of state power and their administrations, the Ministry of Defense and structures of direct subordination to the Minister of Defense designated by the Minister of Defense, and formations of the Bulgarian Army, local self-government bodies and local administration, public legal entities established by law or by an act of an executive authority, natural and legal persons– in which classified information is created, processed, stored or provided.[76]

[76]§1, item 3 of the AP to PPE.

The organizational units are responsible for the direct implementation and compliance with the legal requirements for the protection of classified information and control their compliance; are responsible for the protection of the information and in the case of unregulated access to classified information - take measures to limit the adverse consequences after notifying the SCISM; provide information to the SCIS, to the security services and to the public order services, in accordance with the provisions of the PPE.

Employees working in the organizational units granted access to the relevant level of classified information have a number of obligations - to protect classified information from unregulated access; to immediately notify the information security officer of cases of unregulated access to classified information; to notify the information security officer of all cases of changes to classified materials and documents where unauthorized access is not available; undergo periodic health examinations at least once every two years and psychological examinations.

For those of them who have been cleared to access classified information with a classification level of "Top Secret", the obligation to inform the Information Security Officer in writing of any private foreign travel before the date of departure, unless the travel is in countries with which Bulgaria has concluded agreements for the mutual protection of classified information.

Security and public order officers shall notify their supervisors in writing of any foreign travel.

2.5. Information Security Officer

The head of the organizational unit leads,organizes and supervises the activities for the protection of classified information. He appoints an information security officer to carry out the activity of protection of classified information in the organizational unit after obtaining permission for this person's access to classified information, issued according to the provisions of the Civil Codeand the rules and regulations of the SCISI.

When the volume of work or the level of classified information in the relevant organizational unit is not high, exceptionally, the head of the organizational unit himself can perform the functions of an information security officer.

In cases where the position of a security officer is isolated, then he is directly subordinate to the head of the organizational unit.

PPEestablishes certain requirements for holding the position of "information security officer". A person who is a Bulgarian citizen and has received permission to access the relevant level of classified information in accordance with the procedure established by law can be appointed as such.[77]After appointment, the information security officer must undergo training in the field of protection of classified information.

The duties of the information security officer are specifically listed in the law[78]:

- monitors compliance with the requirements of the law and international treaties in connection with the protection of classified information;
- applies the rules regarding the types of protection of classified information;
- develops a plan for the protection of the organizational unit through physical and technical means and monitors its implementation;
- performs periodic inspections of the reporting and movement of materials and documents;
- conducts research in the cases provided for by law[79];
- carries out the procedure for the ordinary investigation within the organizational unit and keeps a register of the investigated persons;
- notifies the SCIS upon the expiration of the permits, upon the employee's departure or reassignment, as well as upon the need to change the permit related to access to a certain level of classification;

[77]See section 5.6 of this chapter, below.
[78]Art. 22, para. 1 PPE.
[79]Art. 47 PPE.

- informs immediately in writing SCIS and the competent office of any change relating to the circumstances related to the issued permits, certificates, certificates or confirmations;
- keeps a record of cases of unregulated access to classified information and of the measures taken, of which he immediately informs the SCIS;
- monitors the correct determination of the information classification level;
- develops a plan for the protection of classified information in a state of war, military or other emergency;
- organizes and conducts the training of employees in the organizational unit in the field of protection of classified information.

In the event of a change related to the circumstances related to the expiration of the term or other circumstances regarding the issued permits, certificates, certificates or confirmations, as well as in cases of unregulated access, the information security officers of the security and public order services shall notify immediately the heads of services, and those working in the Ministry of Defense, in the structures directly subordinated to the Minister of Defense and the Bulgarian Army, immediately notify the DANS.

2.6. Administrative units on information security

To the extent that the volume of classified information may be large enough to fulfill the tasks and functions of the information security officer, administrative security units may be created for it.

All persons working in these units must meet statutory requirements for an information security officer.

3. Types of classified information

3.1. A state secret

A state secret is classified information defined in a speciallist[80], the unregulated access to which would create a danger for or damage the interests of the Republic of Bulgaria, related to national security, defense, foreign policy or the protection of the constitutionally established order.

In the list defining the scope of information constituting a state secret[81], it is grouped into different categories.

*The first category*covers information related to the defense of the country:

- structure, organization and functioning of the state bodies and the Supreme Command of the Armed Forces of the Republic of Bulgaria in a state of war, military or other emergency.
- location, equipment, maintenance, operation and security organization of the control points of the central and territorial administration of the executive power and the Armed Forces of the Republic of Bulgaria, intended for use in a state of war, military or other emergency.
- organization and functioning of the communication and information systems for the connection of the bodies of state administration and the Armed Forces of the Republic of Bulgaria in various states and degrees of combat readiness and war.
- information on bringing the country to a higher state and degrees of combat readiness, wartime plans and estimates, projects and measures related to ensuring the defense capability at the national level of the central and territorial administration of the executive power and of commercial companies producing military products . Information about

[80]Appendix No. 1 to Art. 25 PPE.

[81]It has been established that the purpose of the special protection of information classified as a state secret is to serve and guarantee the goals and priorities of national security, and not to restrict access to specific information and data for its own sake. Decision No. 9472 of November 16, 2004 of the Supreme Administrative Court under Adm. e. No. 4120/2004

the planning, organization and functioning of the mobilization deployment of the Armed Forces of the Republic of Bulgaria.

- detailed structure of the armed forces, as well as information on the places of their relocation (pre-deployment), the actual name, organization, staff and list numbers of personnel, armaments and management systems of the Armed Forces of the Republic of Bulgaria, of the individual types of armed forces, branches and special forces, units, compounds, regime units and facilities not included in the official exchange of data resulting from the country's international obligations.
- information about the tasks and combat capabilities of the Armed Forces of the Republic of Bulgaria, the individual types of armed forces, branches and special forces, as well as the potential adversary and the planned areas and directions of military operations.
- organization, functioning and technical means of electronic intelligence.
- organization and functioning of the system of bringing the armed forces, the central and territorial administration of the executive power and the obliged legal entities to higher states and degrees of combat readiness.
- strategic and operational documents that set out the armed forces' concepts of warfare and operations.
- information relating to external dangers and threats to the security of the state of a military nature, defense plans, analyzes and forecasts, as well as the resulting decisions and tasks.
- information on the design, testing, production and arming of new types of weapons, combat equipment and ammunition and the mobilization capacities created for their production.
- information on the planning and provision of the general state wartime plan with material, financial and labor resources, as well as the documents regulating this activity.
- organization, deployment, armament, tasks and capabilities of units and intelligence bodies.
- information on the communication system and frequency distribution of the radio communications of the Republic of Bulgaria, which are related to defense and security.

- plans and reports on the allocated and spent material resources related to specific missions and tasks for the defense of the country, determined by an act of the Council of Ministers.
- plans, information and summary data on the state of operational preparation on the territory of the country and the construction of new objects with wartime purpose.
- summary information on the special production of the defense industry, as well as forecasts of development, plans, production capacities, scientific and research units for the realization of orders for armaments, combat equipment, ammunition and military equipment.
- geodetic and cartographic materials and data, digital models and data, raster images, aerial films, aerial photographs and photographic documents that contain information about the type, character, purpose or engineering equipment of the objects and areas relevant to the defense and security of the state.
- tasks of the central and territorial administration of the executive power and the obliged legal entities in a state of war, military or other emergency.
- organization, operation and management of the system for supplying the Armed Forces of the Republic of Bulgaria with material means in a state of war, military or other emergency.
- data on strategic stockpiles of materiel created for wartime.
- summary information on the import and export of armaments, combat equipment and ammunition for the needs of the Armed Forces of the Republic of Bulgaria.
- planning, implementation and results of research activities of particular importance for the defense and security of the Republic of Bulgaria.
- general information about the relief and character (structure) of the sea and river bottom. The elements that determine the hydrological regime of coastal waters in real time (except fairways declared for international navigation). Data on the established places for troops to cross rivers in the Republic of Bulgaria.

*The second category*information constituting a state secret is related to the country's foreign policy and internal security:

- information from the field of foreign policy, unregulated access to which would seriously endanger national security or could damage or create a risk of significant damage to the country's position in negotiations with another country.
- information and documents about the internal political and military situation of other countries, based on unpublished data, the disclosure of which could endanger the national security of the country.
- information on the organization, methods and means of carrying out specific tasks carried out through the operational-search and operational-reconnaissance activities of the security and public order services, as well as data on their special facilities and the information and objects obtained as a result of these activities, as well as and data enabling the identification of persons who assisted or assisted them in these activities.
- detailed organizational and staffing structure of the security services and the Military Police Service under the Minister of Defense, as well as summary data on their personnel, with the exception of summary data for the employees of the Directorate General "Combating Organized Crime" and the Directorate "Internal Security" of the Ministry of the Interior.
- identifying data or data that can assist in the identification of persons who are not employees but cooperate or have cooperated with security services and public order services. Identification data or data that can help to identify employees of the State Intelligence Agency who carry out operational-intelligence activities.
- information about special intelligence means (technical means and/or the means of their application) used in accordance with the legal provisions.
- data on the type, level of supply and qualities of special equipment, weapons, ammunition, protective equipment, devices and materials used by security services, by public order services, by the Specialized Counter-Terrorism Squad of the Ministry of the Interior and by Attorney General's Office of Defense.

- reports, reports, information bulletins, statistical and other data regarding the operational work of security services and public order services.
- detailed organizational and staff structure of the Special Counter-Terrorism Squad of the Ministry of the Interior, plans, reports, reports and other documents containing information related to the implementation of the activities of the Special Counter-Terrorism Squad of the Ministry of the Interior, as well as identity data of the employees of the Specialized Counter-Terrorism Squad of the Ministry of Internal Affairs when exercising their powers under Art. 89, para. 1 of the Law on the Ministry of the Interior.
- detailed organizational and staff structure of the Bureau of Protection at the Prosecutor General, identity data of the employees providing or implementing the special protection measures or the activities under Art. 14, para. 3 of the Law on the Protection of Persons at Risk in Connection with Criminal Proceedings, information on the organization or implementation of special protection, identification data or data that may help to identify endangered or protected persons within the meaning of the same law.
- information on allocated and used budget funds and state property for special purposes related to national security.
- the unified registers of authorizations, certifications, confirmations or refusals of access to classified information and the files on reliability checks, maintained and stored by the State Security Agency.
- the information related to the production and storage of the seals with the image of the state coat of arms, as well as the seals of the state authorities.
- classified information exchanged between the Republic of Bulgaria and international organizations or countries, marked with a security label "Top Secret", "Secret", "Confidential" or equivalent.
- information on the organizational-technical and program protection of the communication and information systems of the bodies of state power and local self-government and their administrations, as well as of their other information processing systems.

- information on the design, construction, supply of equipment and operation of telecommunication, teleinformation and postal networks for the transmission of classified information representing a state secret, used for the needs of the armed forces, security services or organizations for securing these systems and networks.
- passwords and access codes to devices thatcreate, process, store and transfer information marked Top Secret, Secret or Confidential.
- organization, methods and means of cryptographic protection of classified information marked with the symbol "Top Secret", "Secret" or "Confidential"; description and samples of developed or used means for cryptographic protection of such classified information; key materials and classified information protected by cryptographic methods and means.
- information on the transition of the economy from a peacetime to a wartime situation in the various states and degrees of combat readiness of the state and in a state of war.
- information on the preparation, organization and use of rail, road and water transport in bringing the state and the Armed Forces of the Republic of Bulgaria to higher states and degrees of combat readiness.
- information about the organization, methods and means used to protect the classified information representing a state secret.
- information on the purpose, planning and supply of special purpose objects, as well as plans for their defense and security.
- information about persons suspected of carrying out subversive, terrorist or other illegal activities against public order, security, defense, independence, integrity or international standing of the state, received, verified and analyzed by security services and public order services.
- the system of forms and methods of protection, as well as the operational possibilities for the protection of the state border, the activity of border checkpoints, as well as information on anti-terrorist and anti-sabotage actions at the state border.
- summary data relating to the functioning of the system for the protection of classified information constituting a state secret.

- electronic registers and diaries for registration of documents, as well as lists for other materials containing classified information constituting a state secret.
- materials of the Council of Ministers concerning the strategic potential of the state, as well as government strategic orders related to national security and their implementation.
- information about the production technology, as well as separate ways to protect Bulgarian personal documents, banknotes and other securities and means of payment, as well as other protected (against forgery) documents issued by the state authorities and their administrations.
- information about foreign policy plans and tasks, the disclosure of which would damage important interests of the state until the time of their official announcement.
- materials, documents, report notes from international negotiations and consultations, as well as international treaties or parts thereof, if they are classified information.
- organization and functioning of the diplomatic post.
- the security system of the Bulgarian diplomatic and consular missions.
- the tasks of the Bulgarian diplomatic and consular missions during wartime.
- the tasks of guarding foreign diplomatic and consular representations, as well as representations of international organizations in the Republic of Bulgaria during war.
- information and plans under Art. 18a - 18e of the Disaster Protection Act[82].

*The third category*information constituting a state secret is related to the economic security of the country. Such information is:

- documents for negotiations on the conclusion of financial contracts of national importance, the disclosure of which could damage national security.

[82]Pron. SG. no. 102 of December 19, 2006; last change and add. SG. No. 77 of September 18, 2018.

- research work of particularly significant importance for the interests of the national economy, commissioned by state authorities.
- information about technical, technological and organizational decisions, the disclosure of which would threaten to damage important economic interests of the state.
- information about the operation of control and signaling devices, alarm systems and the security regime, the knowledge of which could damage national security.
- political, economic or military information concerning foreign countries received on condition that it will be protected as classified information.
- plans, forecasts and information on the development of the turnover of special equipment, special technologies and special services with other countries.
- information about inventions or utility models determined to be relevant to the security and defense of the country under the Patents Act[83].

As far as the concept of "state secret" does not create ambiguity, given the explicit listing and categorization of the specific information that falls within the scope of this concept, for greater clarity of the law, the legislator has foreseen the need to clarify another concept related to the concept of state secret - "national security". According to the law, this is a dynamic state of society and the state, in which the territorial integrity, sovereignty and constitutionally established order of the country are protected, when the democratic functioning of the institutions and the basic rights and freedoms of the citizens are guaranteed, as a result of which the nation preserves and increases its well-being and develops, as well as when the country successfully defends its national interests and realizes its national priorities.[84]

[83]Refers to the Law on Patents and Registration of Utility Models, Pub. State Gazette, no. 27 of 04/02/1993, in force from 06/01/1993; amend., no. 58 of 18.07.2017, in force since 18.07.2017 (author's note).
[84]See §1, item 13 of the AP to PPE, in accordance with Art. 2 of the Law on the Management and Functioning of the National Security Protection System.

3.2. Official secret

An official secret is that classified information that is created or stored by state bodies or local self-government bodies, which is not a state secret, but unregulated access to which would adversely affect the interests of the state or would damage another legally protected interest.[85]

Such interests of the state are the guarantee of sovereignty and territorial integrity and the protection of the constitutionally established order in the Republic of Bulgaria, including: detection, prevention and counteraction of encroachments against the independence and territorial integrity of the country; uncovering, preventing and countering covert encroachments that harm or threaten the country's political, economic and defense interests; obtaining information about foreign countries or of foreign origin, necessary for decision-making by the highest bodies of state power and state administration; uncovering, preventing and counteracting covert encroachments aimed at forcibly changing the constitutionally established order in the country, which guarantees the exercise of human and citizen rights, democratic representation based on a multi-party system and the activities of the institutions established by the Constitution; detection, prevention and counteraction of terrorist acts, illegal trafficking of people, weapons and drugs, as well as illegal trafficking of products and technologies placed under international control, money laundering and other specific risks and threats.[86]

Information subject to classification as an official secret is diverse and is qualified as an official secret by different laws regulating public relations in individual sectors.

For example. art. 14, para. 4 of the Law on the National Revenue Agency (NRA)[87]determines that an official secret is information regarding the means of protecting tax and social security information and information representing an

[85]Thus, the wording of the concept of "official secret" under Art. 26 PPEis an independent and separate ground for refusal to grant access to public informationunder APIA. Decision No. 162 of January 12, 2004 of the Supreme Administrative Court under Adm. e. No. 8717/2003

[86]See §1, item 14 of the AP to PPE.

[87]Pron. SG. no. 112 of November 29, 2002; last supplement, no. 109 of December 20, 2013, in force since January 1, 2014; last amend., no. 13 of 12.02.2019

official secret, information regarding the design, construction and functioning of information systems and networks for the transmission of tax and social security information, etc. Anyway, par. 1, item 3 of the AP of the Law on the State Agency "National Security" (NSA)[88]determines that an official secret is the information that is not a state secret, but is related to the performance of the functions and tasks of DANS and the realization of the powers of its bodies or is obtained as a result of this activity, unregulated access to which would have a negative impact the interests and security of the state, the activities of the agency, its employees in connection with the performance of their duties or third parties, etc.

The head of the relevant organizational unit, within the framework of the law, announces a list of the categories of information constituting an official secret for the sphere of activity of the organizational unit. The order and manner of announcing the list shall be determined in the regulations for the implementation of the law.[89]

3.3. Foreign classified information

The provisions of the law extend their protectionon foreign classified information. However, to the extent that relevant foreign laws may define classified information with rules and scope that differ from those under Bulgarian law, defining this information as classified is impossible. The legislator limits himself to defining that foreign classified information is the classified information provided by another country or an international organization under an international treaty to which the Republic of Bulgaria is a party.

4. Information Security Classification Levels

Depending on the degree of sensitivity of the informationand its significance to the country's national security and interests, the information is classified into several security categories. Each category is marked with a corresponding label: "For official use", "Confidential", "Secret", "Top Secret" and additional markings.

[88]Pron. SG. no. 109 of December 20, 2007, in force since January 1, 2008; last amend., no. 71 of August 13, 2013, in force since August 13, 2013; last change and supplement, no. 17 of 26.02.2019
[89]See chapter III of the PPZKI.

Information constituting an official secret is marked with the security label "For official use".

The label "Confidential" is placed on information - a state secret, when unregulated accessto it would threaten the sovereignty, independence or territorial integrity of the Republic of Bulgaria or its foreign policy and international relations related to national security, or could create a danger of harm occurring, or cause such harm in the field of national security, defense, foreign policy or the protection of the constitutionally established order.

The next level with higher sensitivity intensity"Secret" means information constituting a state secret when unregulated accessto it would threaten to a high degree the sovereignty, independence or territorial integrity of the Republic of Bulgaria or its foreign policy and international relations related to national security, or could create a danger of difficult to repair or great damage, or cause such damage in the area of national security, defense, foreign policy or the protection of the constitutionally established order.

The label "Top Secret" is placed on information constituting a state secret,in cases where unregulated access would threaten to an extremely high degree the sovereignty, independence or territorial integrity of the Republic of Bulgaria or its foreign policy and international relations related to national security, or could create a risk of incurring irreparable or extremely large damages, or caused such harm in the field of national security, defense, foreign policy or the protection of constitutionally established order.

It is possible to have information - a state secret - of an even more sensitive nature, when the nature of the information or an international treaty to which the Republic of Bulgaria is a party require additional protection. In these cases, the SCIS, at the proposal of the Minister of Internal Affairs, the Minister of Defense or the directors of the security services, may determine by decision additional markings of materials and documents with a higher level of classification than "Top Secret", to establish a special order for the creation, use, reproduction, provision and storage of these materials and documents and determine the circle of persons with the right of access to these materials and documents.

The leveling of security classification levels of foreign classified information received or of classified information provided by the Republic of Bulgaria to another country or international organization in fulfillment of an international treaty entered into force for the Republic of Bulgaria and for the relevant foreign country or international organization is carried out in accordance with the provisions of the contract.

Classified information may not be marked with more than one bar.

5. Marking of information

The marking of classified information constitutes a designationat the appropriate security classification level by entering it into the appropriate objectification form. Marking is done by placing the corresponding security tag.

The security label contains the classification level, classification date, classification expiration date when different from the standard statutory periods, and the legal basis for classification.[90]

When separate or grouped materials and documents contain classified information with different levels of security, a label corresponding to the highest level of classification is placed.

The security tag is determined by the person who has the right to sign the document containing classified information or certifying the presence of classified information in material other than this document. When another person creates the document or material, he is required to put a security stamp with validity until its final determination by the person who has the right to sign it.

Placing, changing, or deleting a security tag is done only within the scope of the individual's access to classified information.

[90]Art. 30, para. 2 PPE.

The law prohibits placing a security tag that does not correspond to the classification level determined by law. For example, information with a classification level of "For official use" cannot be assigned a security label of "Top Secret" and vice versa.

The classification level cannot be changed or removed without the consent of the person who signed it or their superior. Of course, this concerns the person performing the relevant position in the office with access to classified information, and not the specific individual who signed the document.

Changing the classification level without reason is prohibited.

When a designated person who has the right to access classified information finds that the security tag is incorrectly placed and does not correspond to the corresponding level of classification of the information, he is obliged to immediately notify the person who signed the document or his superior.

There is a duty to notify in any case of a change in classification level. Thus, in the event of a change, the recipient of the information and all third parties are always notified by the persons who provided them with information.

The order and way of marking the information is determined by the PPZKI.[91]

6. Storage of classified information - ways and deadlines

6.1. Terms and methods of storage

The creation, storage, processing, provision of access and destruction of classified information is carried out strictlycertain order in the law and depends on its classification level.

[91]See chapter III of the PPZKI.

The total term of protection is one year. After its expiration, the classified information protection authority transfers it to the relevant state archive, unless there is another term established by law.

Only after the expiration of this period can the information be destroyed. This is done after the permission of the SCISM on the proposal of a specially appointed commission with the order of the head of the relevant organizational unit.

When the classified information is acquired through the use of special intelligence means, it is destroyed according to the special procedure provided for this in the Civil Code.[92]

Classified information transferred for storage is protected for a long time. The law stipulates that from the moment of its creation, the information is protected in the following terms:

- information marked with the security label "Top Secret" - 30 years;
- information marked with the security symbol "Secret" - 15 years;
- information marked with the security symbol "Confidential" - 5 years;
- information classified as an official secret – 6 months.

These terms can be extended at most by the time of the initially determined term at the discretion of the State Security Service, when national interests so require. After these terms expire, the classification level is automatically removed and access to this information is carried out in accordance with the GDPR.[93]

When any organizational unit storing classified information ceases to exist, the stored information shall be provided to the SCISM.

[92]Pron. SG. no. 95 of October 21, 1997; last add. SG. No. 37 of May 7, 2019. See chapter four of the SIMA.
[93]See Module 2. above.

6.2. Register of classified information

For all classified information, regardless of its carrier, a special register is maintained by the State Security Agency. The register contains the following data:

- the organizational unit in which the relevant material or document was created;
- the date of creation and the intended date of removal of the classification level;
- the identification number of the material or document under which it appears in the register;
- the legal basis for classification of the material or document and the security bar;
- the change or removal of the classification level and the date of their implementation.

The heads of the organizational units have an obligation to provide the SCISM immediately with the information necessary for entry into the register, as well as to immediately notify the commission of any change in the level of classification or its removal.

An assessment of the need to change the terms and the level of protection of each material is carried out every two years. Obliged persons are those who have the right to sign the document containing classified information or certifying the presence of classified information in material other than this document.

The procedure for providing data for entry in the register, as well as the conditions and procedure for making inquiries from the register, are determined in the PPZKI.[94]

[94]See chapter four of PPZKI.

7. Conditions and procedure for obtaining access to classified information

7.1. Prerequisites for gaining access

Two groups of people have access to classified information- those to whom, on the basis of law, this right has been recognized to a certain extent, and those for whom the position held or the activity performed require them to have access, after carrying out a corresponding reliability study.

Persons who by virtue of law have the right of access to classified information are, first of all, the Speaker of the National Assembly, the President of the Republic of Bulgaria and the Prime Minister. These individuals have the right to access all levels of classified information for the duration of their tenure.

Another group of persons who receive the right of access by the fact of holding the position are the deputy prime ministers, ministers, the chief secretary of the Council of Ministers, people's representatives, judges of the Constitutional Court, judges, prosecutors, lawyers and investigators, members of the Supreme Court council, the chief inspector and the inspectors in the Inspectorate of the High Judicial Council. These individuals are granted access to all levels of classified information for the duration of their tenure on a "need to know" basis, the information being:

- for the deputy minister, the presidents, the ministers and the chief secretary of the Council of Ministers - within the scope of their competence;
- for the people's representatives - when a decision of a parliamentary committee or the National Assembly is taken according to the established procedure, or when a committee or the National Assembly is sitting in closed session;
- for judges, prosecutors, lawyers and investigators - only for the specific case;
- for the members of the Supreme Judicial Council - upon a decision taken according to the established procedure by the relevant collegium

or the plenary session of the Supreme Judicial Council, when the collegium or the plenary session is sitting in closed session;

- for the chief inspector and for inspectors in the Inspectorate of the Supreme Judicial Council - when exercising their powers.

No background check is conducted for all individuals who are legally entitled to access classified information. Also, a reliability investigation is not carried out on individuals in or in connection with the exercise of their constitutional right to protection.

For example, if a person is charged with the disclosure of classified information or another crime related to access to such information, they must be able to conduct the defense afforded to them by law. If that protection were predicated on clearances to access classified information, that person's ability to defend would be thwarted. In this case, the constitutional right to protection has a higher intensity and priority over the right to access classified information.

For all other persons, with the exception of cases where information classified as an official secret is accessed, a reliability study is carried out.[95]Based on the investigation, a clearance to access classified information is issued.

7.2. Conditions for obtaining access

For an individual to gain access to classified information, it must meet two sets of conditions.

From the point of view of his citizenship, educational qualifications, legal and health status, he must have Bulgarian citizenship (except for cases of granting access based on an international treaty), be of legal age, have completed secondary education, not be convicted of an intentional crime of a general nature, regardless

[95]See Fetti, N. Termination of contracts related to access to classified information. //Commercial and competition law, no. 3, March 2009, p. 23 - Access to classified information is granted on a "need to know" basis to persons who have undergone a reliability investigation procedure and have been issued a corresponding act of access - authorization to access, security certificate, confirmation, certificate.

of rehabilitation, be reliable from the point of view of security and secrecy and not suffer from mental illnesses certified in the relevant order.

From the point of view of reliability, the person must have no evidence of carrying out activities against the interests of the Republic of Bulgaria or against interests that the Republic of Bulgaria has undertaken to protect under international treaties, must not have participated in espionage, terrorism, sabotage or subversive activity, did not carry out any other activity against the national security, territorial integrity or sovereignty of the country or aimed at a violent change of the constitutionally established order and did not carry out any activity directed against public order.

Additional criteria for establishing the reliability of the person, from the point of view of protecting secrecy, are the absence of data regarding the concealment or giving of false information by the person under study for the purposes of the study, facts and circumstances that would make it possible to blackmail the person under study, discrepancy between the subject's standard of living and his income, mental illness or other disorders of mental activity that would negatively affect the subject's ability to work with classified information, and the subject's addiction to alcohol and drugs.

To the extent that the establishment of certain facts and circumstances regarding the state of health cannot be carried out from already collected data, the body conducting the study may request that the person being studied undergo specialized medical and psychological examinations and present their results in institutions and on order determined by regulation.[96]The subject has the right to refuse to undergo the requested specialized medical and psychological examinations. The refusal is made in writing and the study is terminated.

[96]See Ordinance No. 6 of March 19, 2003 of the Minister of Health on the procedure and places for carrying out specialized medical and psychological examinations and periodic health examinations and the methods of their conduct; Pron. SG. no. 35 of April 16, 2003

7.3. Research procedure

The survey procedure is regulated in detail in RILPCI.[97]Depending on the access allowed, different types of studies are carried out, in terms of their depth and the methods used:

- ordinary research - for access to classified information with a classification level of "Confidential";
- advanced research - for access to classified information with a classification level of "Secret";
- special investigation - for access to classified information with a classification level of "Top Secret".[98]

The law sets deadlines for the completion of reliability investigations - for the ordinary investigation it is up to 30 days from receipt of the written order or request, for the extended investigation - up to 45 days, and for the special investigation - up to 60 days. These deadlines may be extended by the relevant managers, but not by more than 20 days, based on a reasoned written request from the security and public order officers or the information security officers conducting the investigation. In case of established affiliation to the State Security and to the intelligence services of the Bulgarian People's Army, the terms under para. 1 are extended by 15 days.

The investigation procedure ends with the issuance of a special authorization for access to classified information for the appropriate level by the SCISM, the security services or an information security officer.

7.4. Issuance, revocation, termination and refusal to issue an access permit

The access permit is a written document and is issued in threethe copy according to the model approved by the State Security Agency.

[97]See chapter six, section II of PPZKI.
[98]Regarding the methods and prerequisites for carrying out the various types of studies, see Art. 47 – 51 of the Civil Code.

The permit entitles the person for whom it is issued to the relevant level of qualification. If an authorization for access to a higher level has been issued, the authorization gives the right to access to classified information of a lower level, if this access is required in connection with the position held or the performance of a specifically assigned task.

The access permit is issued for a certain period. This term is 5 years for the Confidential classification level, 4 years for the Secret classification level, and 3 years for the Top Secret classification level. Before the expiration of these terms, in order to issue a new permit, a new survey is carried out according to the order specified in the previous section.

A refusal to issue permission for access to classified information from the relevant level is made when, in the course of the study, it is established that the person does not meet any of the requirements for granting access to classified information under Art. 40, para. 1 of the Civil Code or in the presence of falsely declared facts and circumstances.[99]A subject who has been denied permission to access classified information is not entitled to apply for a position or to perform a specific task related to work with classified information of the same or higher classification level for a period of one year from the issuance of the refusal.

The validity of the authorization may be limited or revoked. This happens in the presence of several hypotheses. First of all, it is possible for a person for whom a permit has been issued that new facts and circumstances become known that cast doubt on his reliability. In this case, a check of these facts and circumstances is carried out and after receiving the results from the head of the organizational unit, he can limit the access of the researched person to the corresponding level of classified information, promptly notifying the authority that issued the authorization.

[99]According to Art. 58 PPEpermission and refusal to issue permission for access to classified information contain precisely defined details - authority that issued the document, name, surname, surname, date and place of birth and TIN of the person under study, type of study, level of information security classification , to which access is permitted or denied, legal basis for issuing or refusing to issue a permit for access to classified information, validity period of the permit, permit or refusal number, date and place of issuance, signature and stamp.

The permit may be revoked by the authority that issued it, when the inspection has established that the person does not meet any of the requirements for providing access to classified information under Art. 40, para. 1 LLCI or has committed a violation of the law or the by-laws on its implementation, which has created a danger of occurrence or has led to significant damage to the interests of the state, organizations or individuals in the field of protection of classified information, as well as when the person has committed systematic violations of the law or the by-laws related to the protection of classified information. The person whose access permission has been revoked has no right to apply for a position or to perform a specific task related to working with classified information for a period of three years from the revocation.

The termination of the permit should be distinguished from its withdrawal. Termination is the suspension of the operation of an issued permit based on a written proposal of the information security officer in the presence of circumstances and facts of an objective nature. Such are death of the person granted access to classified information, expiration of the terms of the authorization, change of the need for access to a higher level of information security classification, and loss of the need for access to classified information.[100]

The refusal to issue a permit for access to classified information, as well as the termination or revocation of an issued permit, may be appealed to the SCISM according to the administrative procedure specified in the law.[101]The decision of the SCISM is subject to appeal before a three-member panel of the Supreme Administrative Court.

The refusal, termination and revocation of an issued authorization for access to classified information, issued by the DSSI, are also subject to appeal before a three-member panel of the Supreme Administrative Court. The court's decision is final.

[100]Termination of permission to access classified information, including on the basis of Art. 60, para. 1, item 4 of the Civil Code- upon expiry of its term, it does not happen automatically with the expiry of this term, but is carried out by an express written act of the authority that issued the permit. Ruling No. 1207 of September 26, 2011, pursuant to City Decree No. 1168/2011 of the Supreme Court of Cassation.
[101]Art. 63 – 67 of the Civil Code.

Cases are created for all reliability studies and materials created or collected on them. These files are stored, maintained, updated, filed and closed by the investigating authority separately from other types of files. The management and storage of these files is governed by the PPZKI.[102]

8. Types of protection of classified information

Protecting classified information is complexof organizational, physical and technical measures to prevent unregulated access to materials, documents, equipment and facilities classified as state or official secrets.

These measures can be tentatively considered in several directions.

8.1. Physical security

Physical security includes the protection of the buildings, premises and facilities in which classified information is created, processed and stored, and the control of access to them against unregulated access or influence (for example, an act of terrorism).

The necessary methods and means for physical security are determined depending on the level of classification and the amount of classified information, on the number and level of access of workers and employees with access, on the degree of threat of damaging actions, etc. For this purpose, heads of organizational units, with the help of information security officers, determine security zones (for access), control zones, establish a controlled mode of entry, movement and exit from security zones, technical control and protection of zones , a mode for storing keys to premises, cash registers and other facilities used to store classified information and the like.

When the goal is to ensure the protection of classified information representing a state secret, additional protection measures are established in the law. Thus, during meetings, conversations, conferences, meetings, etc. additional

[102]See Art. 151 – 156 PPZKI.

security measures against eavesdropping and surveillance are introduced. Persons participating in such meetings shall be vetted in advance by the security and guard units in the organizational unit.

The materials and technical means that are used to protect classified information are subject to certification forstability and indestructibility corresponding to the security classification level. The certification is carried out by the DSSI or by another body determined by a decision of the Council of Ministers.[103]

The means of physical security certified for each level of security classification are defined in a list approved by the SCISM[104], and the system of measures, methods and means for physical security, the conditions and order for their use are determined by an ordinance of the Council of Ministers.[105]

Information security officers perform preliminary and ongoing controls regarding the organization, capabilities and means of physical security in the organizational unit.

8.2. Document security

When the classified information is related to the creation, processing and storage of documents, a system of measures, methods and means for document security, determined by the PPZKI, is applied.[106]

Each head of an organizational unit may, within his competences, determine other additional special procedures and requirements regarding documents.

For the needs of accountability and the prevention of illegal export, destruction, processing, knowledge and access to documents containing classified information, a separate unit - registry is created for each organizational unitfor

[103]Art. 77, para. 1 PPE.
[104]Art. 77, para. 3 PPE.
[105]Art. 78 PPE.
[106]Art. 80, para. 2 PPE.

classified information. Special registers document the creation, processing, storage and transfer to authorized persons of materials containing classified information. The units are directly subordinated to the information security officer.

The requirements for the construction and operation of the registries are regulated in the PPZKI.[107]

8.3. Personal security

The system of principles and measures that are applied by the competent authorities to persons working with classified information, in order to guarantee their reliability and with a view to protecting the information, is called personal security.[108]

The principles and measures include ensuring access to classified information only with a view to the necessary information for the implementation of their powers - the so-called "need to know" principle.

These measures also include the investigation procedure for issuing an access permit, the conduct of trainings for working with classified information, the control over the activities of persons working with classified information and others, defined in the PPZKI.[109]

8.4. Cryptographic security

For preventing knowledge of classifiedinformation from unauthorized persons, various cryptographic methods and means of its protection are applied. The conditions and order for the use, production and import of cryptographic methods and means of protection of classified information are determined by the

[107]Art. 82, para. 2 PPE.
[108]Art. 83, paragraph 1 of the Civil Code.
[109]Art. 83, para. 2 PPE.

Ordinance on the Cryptographic Security of Classified Information (OCSCI), adopted by the Council of Ministers.[110]

The application of these cryptographic methods and means is related to the use of mathematical algorithms of symmetric and/or asymmetric cryptography, which are usually not secret, but the cryptographic keys used in the encryption and decryption process are secret. In this regard, the creation and provision of the cryptographic keys is carried out by the DSSI, and the use of the relevant methods and means is allowed only after prior approval and registration by the commission.

Within the relevant organizational unit, the application of cryptographic methods and means is carried out by the information security officer or by other employees from the security administrative unit, who have undergone training in the field of cryptographic security and received a special permit from the SCISM to work with cryptographic means. Issuance, termination and revocation of permission is carried out under the conditions and according to the order of issuance of permissions to work with classified information. Refusal, termination and revocation are not subject to judicial appeal. They are subject to an administrative appeal before the SCIS according to the procedure for appealing refusals to issue a permit to access classified information, as well as the termination or revocation of an issued permit (see Topic 19 above).

Training in cryptographic security is conducted by DANS or by other organizational units after permission and under its control.

8.5. Security of communication and information systems

As a significant part of the classified information is subject to automated processing and transmitted electronically, it is necessary to provide a system of adequate principles and measures to protect against unregulated access to this information when it is created, processed, stored and transferred through the communication and information systems (ICS).

[110]Pron. SG. no. 102 of November 21, 2003; last change and supplement, no. 35 of 10.05.2016, in force from 10.05.2016.

The mandatory general conditions for CIS security cover computer, communication, cryptographic, physical, documentary and personal security, CIS connection security, security of the information itself on any electronic medium and TEMPEST countermeasures. They are defined in an ordinance adopted by the Council of Ministers on the proposal of the chairman of the National Academy of Sciences.[111]

Heads of organizational units may define specific security requirements for systems and networks within the organizational unit, but only after their approval by DANS. The specific requirements may cover security measures right from the moment of designing the relevant information system or network, as well as measures related to their operation.

The state-organized control by DANS covers a complex assessment of the security of the relevant system and network before putting it into operation. A security certificate is issued for the performed assessment. It is not allowed to create, process, store and transfer classified information in CIS without having a certificate issued for them.

Internal organizational control of departmental systems and networks for compliance with security requirements is carried out by the head of the organizational unit. However, he can assign control to specific employees from the security unit or to the information security officer himself.

In order to prevent external interventions and to minimize the risks of external interventions in CIS intended for the creation, processing, storage and transfer of classified information, the law introduces special rules regarding the connection of CIS to public networks such as the Internet:

- An intersystem connection of CSIs intended for classified information up to and including the "Secret" level is allowed with other CSIs for classified information with the same or a different classification level,

[111]Ordinance on the mandatory general conditions for the security of automated information systems or networks in which classified information is created, processed, stored and transferred (NZOUSAISMSSOSPKI); Pron. SG. no. 46 of May 20, 2003; last change and supplement, no. 35 of 10.05.2016, in force from 10.05.2016.

as well as to information systems of a closed type under the conditions specified in НЗОУСАИСМСОСПКИ;

- An inter-system connection of CIS intended for classified information with the "For official use" level to the Internet or other public networks is allowed under the conditions specified in the HZOUSAISMSSOSPKI;
- Intersystem connection of CSIs intended for classified information at the level of "Confidential" and "Secret" with CSIs intended for classified information at the level "For official use" that are connected to the Internet or other public networks is not allowed.
- Intersystem connection of CSIs intended for classified information with the level of "Top Secret" is not allowed.

8.6. Industrial security

The use and handling of classified informationrequires the use and delivery of various technical and cryptographic equipment, creation of CSI, equipment for providing physical barriers to access, creation of special premises, educational events, provision of repair activities, etc., for which the relevant authorities need to conclude contracts with external suppliers - individuals and legal entities. Industrial security is the system of principles and measures that apply to these external suppliers with a view to protecting classified information from unregulated access.

The requirements for guaranteeing industrial security are determined by an ordinance of the Council of Ministers.[112]

At the proposal of the SCISM, the Council of Ministers determines by decision the body conducting the investigation procedure and issuing a security certificate. Contracts with external suppliers define the specific requirements for the protection of classified information, related to the volume and level of security

[112]Ordinance on the general requirements for guaranteeing industrial security; Pron. SG. no. 22 of March 11, 2003, in force since March 11, 2003, amended, no. 24 of March 14, 2003, amended. and supplement, no. 104 of December 11, 2007

classification, the persons having access to it, liability clauses in case of non-compliance with industrial security requirements, etc.

When it is necessary to provide classified information to such persons, an access permit must be issued for individuals, and an access certificate for legal entities.

In order to obtain a certificate, a survey of the applicant is carried out, during which data is collected on the persons holding managerial positions, as well as on the persons who are entrusted with the immediate execution of the contract, on the persons involved in conducting the negotiations in connection with the conclusion of the contract , on the persons working in the applicant's security administrative unit, on the structure and origin of the applicant's capital, commercial partners, financial relationships, property rights and other data necessary to assess the reliability of the applicant.

A certificate of access to classified information is issued only when the applicant meets the security requirements under the PPE and the acts on its implementation, and is economically stable[113], and is reliable from a security point of view[114]. Economic stability is verified by evidence and affidavits issued by the relevant authorities within their competences, and the applicant's reliability from a security point of view is carried out through an investigation by the security services.

Depending on the result of the conducted investigation, the authority that carries it out issues a security certificate or decides to refuse its issuance.

[113]According to Art. 101 PPEis not an economically stable applicant who: has been declared bankrupt or is in bankruptcy proceedings; is adjudged bankrupt; is in liquidation; is deprived of the right to exercise commercial activity; has a liquid and demandable obligation to the state, to insurance funds, as well as to individuals or legal entities, when it is recognized before the enforcement authority or when it is established by an effective court decision, by a notarized document or by a security issued by third person; has been convicted with an effective sentence for a crime against property or against the economy, unless he has been rehabilitated. The last requirement also applies to the managers, respectively to the members of the management bodies of the candidates.

[114]Reliability requirements are defined in Art. 102 PPE- they are the same as for persons working with classified information (Art. 41 PPE), but the specified research candidates must also meet the security requirements under Art. 40 of the Act. In the latter case, the applicant may propose other persons who meet the reliability requirements.

The security certificate is issued for a period of no longer than three years, and if it is necessary to extend it, a check for economic stability and reliability is carried out again. A new investigation is not carried out on individuals or legal entities who, during the period of the issued security certificate, apply for the performance of another contract related to access to classified information of the same or lower information security classification level for which they received security certificate.

If, in the process of performing the work, one of the persons who received a security certificate ceases to meet the requirement of economic stability or reliability, if the defect is repairable, the body that issued the certificate sets a deadline for eliminating the deficiencies. If the defects are not removed within the given period or are irremediable, as well as in cases where they led to unregulated access to classified information, the certificate is revoked.

The refusal to issue a certificate, as well as its revocation, are not subject to judicial appeal. They appeal only to the SCIS.[115]

The data collected during the study of applicants for the issuance of permits and certificates are stored by the authority that carried out the study in special cases, and the collected information is protected as classified information. A special term has been set for the storage of these files - 20 years, counted from the date of termination of the applicant's activity. The opening, storage, maintenance, updating, filing and closing of reliability study cases are defined in the PPZKI.[116]

When a contract supplier related to classified information has received a security clearance, it has all the obligations of an organizational unit.[117]

The protection of classified information in the field of inventions and utility models is carried out in accordance with the provisions of the Patent Law[118], unless the ŽPKI provides otherwise.

[115]See Topic 19. above.
[116]See Art. 151 – 156 PPZKI.
[117]See Topic 14. above.
[118]This refers to the Law on Patents and Registration of Utility Models (author's note).

9. Trends in the development of the EU legislation for regulation of classified information and its impact on the Bulgarian legislation

A few general trends in the development of the EU legislation which could impact the regulation of classified information in Bulgaria could be outlined.

9.1. Digital Market Act impact

The Digital Market Act (DMA) represents a significant shift in the EU's regulatory landscape, particularly affecting digital platform ecosystems. It act aims to foster fair competition and innovation within the digital market.

The DMA could have implications for how classified information is managed on digital platforms, especially concerning data sharing, interoperability, and the use of personal data. It's poised to introduce new rules for large tech companies, impacting how they handle user data and ensuring they do not misuse their market dominance.[119]

This regulation underscores the EU's commitment to protecting consumer rights in the digital age and addresses the challenges posed by the growing influence of tech giants. The focus is on creating a more level playing field, promoting innovation, and safeguarding user privacy and classified information.

9.2. Change in European digital policy

Some authors indicate a notable shift in the EU's digital policy following the introduction of the 2015 Digital Single Market Strategy. This shift focuses more on defense against digital threats rather than solely on promoting liberalization.[120]

This change could directly impact the regulation of classified information, as it suggests a more cautious and protective approach to digital assets and

[119] Heimburg, Vincent, and Wiesche, Manuel. Digital platform regulation: Opportunities for information systems research. Internet Research. 2023. (https://www.emerald.com/insight/content/doi/10.1108/INTR-05-2022-0321/full/html).

[120] Savin, A. The change in direction of the European digital policy on the content layer after the introduction of the 2015 Digital Single Market Strategy. (https://scindeks.ceon.rs/Article.aspx?artid=2217-28152001093S).

information security. It reflects a growing awareness of cyber threats and the need for robust digital defenses.

The policy shift may lead to stricter regulations on data handling, cybersecurity measures, and cross-border data flows, all of which are crucial for maintaining the integrity and confidentiality of classified information within the EU.

9.3. Transparency rules for clinical trials

The EMA is revising its transparency rules for clinical trials. This revision aims to balance the need for public access to clinical trial data with the protection of classified information, such as commercial confidential information and personal data.[121]

The upcoming regulations will likely influence how pharmaceutical companies and research institutions handle and disclose clinical trial data. This could include new guidelines for data anonymization, sharing, and publication, ensuring that sensitive or classified data is adequately protected.

This regulatory change highlights the EU's commitment to both transparency in healthcare and the protection of sensitive information. It is a response to the evolving landscape of medical research, digital data management, and public health interests.

9.4. Attitudes and expectations concerning privacy

There's an emerging need for new regulations as public attitudes and expectations about privacy rapidly evolve. The current framework may no longer be sufficient to address the complexities of digital data, including classified information.

This trend suggests that future regulations will need to be more adaptive and responsive to societal changes and technological advancements. It may lead to

[121] González-Quevedo, R., Pioppo, Laura, Garcia Burgos, J., Arlett, P. Reshaping transparency rules for clinical trials by the European Medicines Agency. British Journal of Clinical Pharmacology. 2023 (https://bpspubs.onlinelibrary.wiley.com/doi/10.1111/bcp.15825).

more comprehensive and nuanced laws governing data privacy, cybersecurity, and information classification.

The changing landscape reflects the dynamic interplay between technology, public perception, and legislative action. It underscores the need for ongoing dialogue and collaboration between policymakers, industry stakeholders, and the public.

9.5. Distributed ledger technologies and crypto-assets

The EU is preparing to regulate distributed ledger technologies and crypto-assets. These emerging technologies present new challenges and opportunities for managing and classifying information.[122]

The regulation aims to create a safe and innovative environment for these technologies while ensuring digital-financial security. It will likely address issues like the classification of crypto-assets, consumer protection, and the use of blockchain for secure information management.

This regulatory effort is part of the EU's broader strategy to embrace digital innovation responsibly. It reflects a balanced approach to nurturing technological advancement while safeguarding against risks associated with digital assets and classified information.

These points collectively paint a picture of an EU increasingly focused on balancing innovation with information security, privacy, and the safe handling of classified information in the digital age.

[122] Sevim, Hasret Ozan. Upcoming regulations in the EU on distributed ledger technologies and crypto-assets. Conference paper. (https://dblp.org/rec/conf/dlt2/Sevim23.html).

REFERENCES

1. **Alexandrov, A.** New forms of employer control. Can the electronic correspondence of the staff be subject to control by the employer? // Labor and law, no. 4, April 2012. URL: <http://trudipravo.bg/kokutorni-produkti-epi/kokutorni-informacionni-produkti-epi/epi-trud-i-sotzialno-osiguryavane/podbrani-statii/1742-novi-formi-na-rabotodatelski-kontrol-mozhe- li-elektronnata-korespondentziya-na-personala-da-bade-obekt-na-kontrol-ot-strana-na-rabotodatelya> (24.10.2019)

2. **Alexandre de Streel & P. Larouche** on Regulation of Digital Networks and Services: de Streel, A., & Larouche, P. (2016). Digital Networks and Services: A Specific Regulatory Framework (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728874).

3. **Alexandre de Streel & Christian Hocepied** on EU Regulation of Telecommunications Networks and Services: Streel, A. D., & Hocepied, C. (Reference Year Not Available). EU Regulation of Electronic Communications Networks and Services (https://china.elgaronline.com/edcollchap/edcoll/9781786439321/9781786439321.00013.xml).

4. **Buttow, C. V., & Weerts, S.** (2022). The development of the European Union regulatory framework governing the availability, sharing, and reuse of public sector data (https://journals.sagepub.com/doi/10.1177/20539517221124587).

5. **Dimitrov, G.** Right to information and communication technologies. Part II. Administrative legal and technological aspects, Electronic management. Legal regime of information. Legal Regime of Cryptography. Standardization in the field of ICT. Sofia, Law and Internet Foundation, 2014.

6. **Drexl, J.** (2014). The European Framework for the Regulation of PSI in Terms of Competition

(https://china.elgaronline.com/edcollchap/edcoll/9781784714970/9781784714970.00013.xml).

7. **Definition** No. 1207 of September 26, 2011, in accordance with city decree No. 1168/2011 of the Supreme Court of Cassation.

8. **González-Quevedo, R., Pioppo, Laura, Garcia Burgos, J., Arlett, P.** Reshaping transparency rules for clinical trials by the European Medicines Agency. British Journal of Clinical Pharmacology. 2023 (https://bpspubs.onlinelibrary.wiley.com/doi/10.1111/bcp.15825)

9. **Pavlov, G.** Problems of security and protection of classified information in automated information systems and networks. // Economic Alternatives, UNSS, National and Regional Security Department, no. 5/2005. URL: <http://alternativi.unwe.bg/alternativi/index.php?nid=5&hid=72> (24.10.2019)

10. **Article 29 Personal Data Protection Working Party.** Guidance on consent in accordance with Regulation 2016/679, adopted on 28 November 2017, last revised and adopted on 10 April 2018, WP259 rev.01.

11. **Answer** No. 13947 of November 19, 2010 of the Supreme Administrative Court under adm. e. No. 2357/2010

12. **Answer** No. 162 of January 12, 2004 of the Supreme Administrative Court under adm. e. No. 8717/2003

13. **Answer** No. 2 of 12.02.2015 of the Constitutional Court of the Republic of Bulgaria under Art. e. No. 8/2014, with which the old version of the Law of the European Union (Art. 250a - Art. 250e, Art. 251 and Art. 251a of the Law of the European Union)

14. **Answer** No. 2008 of February 16, 2010 of the Supreme Administrative Court under adm. e. No. 4930 / 2009

15. **Answer** No. 2470 of February 20, 2013 according to Adm. d. No. 4596/2012 of the Supreme Court

16. **Answer** No. 3327 of March 15, 2010 of the Court of Appeal under adm. e. No. 7481/2009

17. **Answer** No. 4962 of April 8, 2011 of the Court of Appeal under adm. e. No. 9086/2010

18. **Answer** No. 8512 of June 13, 2012 under Adm. e. No. 9701/2011 of the Supreme Court

19. **Answer** No. 9472 of November 16, 2004 of the Supreme Administrative Court under adm. e. No. 4120/2004

20. **Answer** of the Court of Justice of the European Union in cases C-293/12 and C-594/12 of April 8, 2014.

21. **Fetty, N.** of contracts related to access to classified information. // Commercial and competition law, no. 3 March 2009.

22. **Heimburg, Vincent, and Wiesche, Manuel**. Digital platform regulation: Opportunities for information systems research. Internet Research. 2023. (https://www.emerald.com/insight/content/doi/10.1108/INTR-05-2022-0321/full/html).

23. **J. Hoboken** on Fragmentation in European Privacy Law and Policy: Hoboken, J. (2014). European Privacy Law and Policy: A Critical Assessment (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418636).
24. **Janssen, K.** Legal Regulation of Access to Public Sector Information. (https://link.springer.com/chapter/10.1007/978-3-030-23665-6_27).
25. **Koerten, H., & Veenswijk, M.** (2013). Organizational Consequences of Policies on the Reuse of Public Sector Information in Europe. (https://content.iospress.com/articles/journal-of-e-governance/gov00356).
26. **Marx, A., & Loo, G**. (2021). Shape of Transparency in EU Trade Policy: A Focus on Free Trade Agreements. Politics and Governance, 9 (1) (https://dx.doi.org/10.17645/PAG.V9I1.3771 https://www.cogitatiopress.com/politicsandgovernance/article/view/3771).
27. **R. Wong & Daniel B. Garrie** on Regulation of VoIP Services and Privacy: Wong, R., & Garrie, D. B. (2009). Regulation of VoIP Services: Bridging

the Gap Between Traditional Telephony and Electronic Communications (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1466153).

28. **Richter, H.** (2018). Including Public Research and Educational Establishments within the Scope of the Directive regulating the re-use of public sector information ('PSI Directive') (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090337).
29. **Savin, A.** The change in direction of the European digital policy on the content layer after the introduction of the 2015 Digital Single Market Strategy. (https://scindeks.ceon.rs/Article.aspx?artid=2217-28152001093S).
30. **Sevim, Hasret Ozan.** Upcoming regulations in the EU on distributed ledger technologies and crypto-assets. Conference paper. (https://dblp.org/rec/conf/dlt2/Sevim23.html).
31. **Tsekov, B.** Access to public information. // Weekly Legalist, no. 31 July 31 - August 6, 2000
32. **Determann, L., Sprague, R.** Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States, 26 Berkeley Tech. LJ 979, 2011. URL: <http://scholarship.law.berkeley.edu/btlj/vol26/iss2/3> (24.10.2019)

NORMATIVE AND OTHER LEGAL ACTS

1. Administrative Procedure Code, Pub. SG. no. 30 of April 11, 2006, final change SG. no. 36 of May 3, 2019;
2. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of the right to privacy in the electronic communications sector (Directive on the right to privacy and electronic communications), Pron. OJ L 201, 31.7.2002, p. 37–47;
3. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data created or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/ EO, Pron. OJ L 105, 13.4.2006, p. 54–63;
4. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing a European Code for Electronic Communications (Revised), Pub. OJ L 321, 17.12.2018, p. 36–214;
5. European Convention on Access to Official Documents - adopted on 27 November 2008 by the Committee of Ministers of the Council of Europe;
6. Law on Administrative Violations and Penalties, Pub. SG. no. 92 of November 28, 1969, final add. SG. no. 83 of October 22, 2019;
7. Administration Law, Pub. SG. no. 130 of November 5, 1998, final add. SG. no. 80 of September 28, 2018;
8. Law on State Agency "National Security", Pub. SG. no. 109 of December 20, 2007, final change and add. SG. no. 17 of February 26, 2019;
9. Law on Electronic Identification, Pub. SG. no. 38 of May 20, 2016, final change SG. no. 58 of July 23, 2019;
10. Law on Electronic Communications, Pub. SG. no. 41 of May 22, 2007, final change and add. SG. no. 74 of September 20, 2019;
11. Law on the electronic document and electronic authentication services, Pub. SG. no. 34 of April 6, 2001, final change SG. no. 58 of July 23, 2019;
12. Law on e-Government, Pub. SG. no. 46 of June 12, 2007, final change and add. SG. no. 94 of November 13, 2018;
13. Law on Protection of Classified Information, Pub. SG. no. 45 of April 30, 2002, final change SG. no. 17 of February 26, 2019;

14. Competition Protection Act, Pub. SG. no. 102 of November 28, 2008, final change SG. no. 28 of April 5, 2019;
15. Law on the Protection of Persons at Risk in Criminal Proceedings, Pub. SG. no. 103 of November 23, 2004, final change SG. no. 17 of February 26, 2019;
16. Personal Data Protection Act, Pub. SG. No. 1 of January 4, 2002, final change and add. SG. no. 17 of February 26, 2019;
17. Disaster Protection Act, Pub. SG. no. 102 of December 19, 2006, final change and add. SG. no. 77 of September 18, 2018;
18. Cybersecurity Act, Pub. SG. no. 94 of November 13, 2018;
19. Law on the Ministry of Internal Affairs, Pub. SG. no. 53 of June 27, 2014, final change and add. SG. no. 58 of July 23, 2019;
20. Law on the National Revenue Agency, Pub. SG. no. 112 of November 29, 2002, final change SG. no. 13 of February 12, 2019;
21. Law on the National Archives Fund, Pub. SG. no. 57 of July 13, 2007, final add. SG. no. 17 of February 26, 2019;
22. Public Libraries Act, Pub. SG. no. 42 of June 5, 2009, final add. SG. no. 94 of November 13, 2018;
23. Law on Patents and Registration of Utility Models, Pub. SG. no. 27 of April 2, 1993, final change SG. no. 58 of July 18, 2017;
24. Law on Prevention and Determination of Conflict of Interest, Pub. SG. no. 94 of October 31, 2008, repealed SG. no. 7 of 19 January 2018;
25. Law on Combating Corruption and Confiscation of Illegally Acquired Property, Pub. SG. no. 7 of January 19, 2018, final change SG. no. 83 of October 22, 2019;
26. Law on Public Finances, Pub. SG. no. 15 of February 15, 2013, last change and add. SG. no. 91 of November 14, 2017;
27. Special Intelligence Means Act, Pub. SG. no. 95 of October 21, 1997, final add. SG. no. 37 of May 7, 2019;
28. Law on the Management and Functioning of the National Security Protection System, Pub. SG. no. 61 of 11 August 2015, final change SG. no. 94 of November 13, 2018;
29. Convention for the Protection of Human Rights and Fundamental Freedoms, ratified by the Republic of Bulgaria with the Law on the Ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms and

the Additional Protocol to it dated 20.03.1952, Promulgated SG. no. 66 of 14 August 1992;
30. Constitution of the Republic of Bulgaria, Pub. State Gazette, no. 56 of July 13, 1991, final change and add. SG. no. 100 of December 18, 2015;
31. Ordinance No. 6 of March 19, 2003 of the Minister of Health on the procedure and places for carrying out specialized medical and psychological examinations and periodic health examinations and the methods for their implementation, Publ. SG. no. 35 of April 16, 2003;
32. Ordinance on the mandatory general conditions for the security of automated information systems or networks in which classified information is created, processed, stored and transferred, Pron. SG. no. 46 of May 20, 2003, final change and add. SG. no. 35 of May 10, 2016;
33. Ordinance on the cryptographic security of classified information, Pron. SG. no. 102 of November 21, 2003, final change and add. SG. no. 35 of May 10, 2016;
34. Ordinance on the exchange of documents in the administration, Pub. SG. no. 48 of May 23, 2008, final change SG. no. 5 of January 17, 2017;
35. Ordinance on the general requirements for guaranteeing industrial security, Pron. SG. no. 22 of March 11, 2003, final change and add. SG. no. 104 of December 11, 2007;
36. Ordinance on the procedure for carrying out inspections for the implementation of direct control on the protection of classified information, Pron. SG. no. 19 of February 28, 2003, final change and add. SG. no. 44 of May 9, 2008;
37. Ordinance on the standard conditions for the reuse of information from the public sector and for its publication in an open format, Pron. SG. no. 48 of June 24, 2016;
38. General requirements for the implementation of public electronic communications, issued by the Commission for the Regulation of Communications, Pron. SG. no. 24 of March 4, 2008, final change SG. no. 10 of February 1, 2019;
39. Regulations for the implementation of the Law on the Protection of Classified Information, Pub. SG. no. 115 of December 10, 2002, final change and add. SG. no. 68 of August 22, 2017;
40. Regulation No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 on public access to documents of the European Parliament, the Council and the Commission, Pub. OJ L 145, 31.5.2001, p. 43–48;

41. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures on access to the open internet and amending Directive 2002/22/EC on universal service and users' rights in relation to electronic communications networks and services and of Regulation (EU) No. 531/2012 on roaming in public mobile communication networks within the Union, Pron. OJ L 310, 26.11.2015, p. 1–18;
42. Regulation (EU) 2016/679 of the European Parliament and of the 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 repealing Directive 95/46/EC (General Regulation on data protection), Pub. OJ L 119, 4.5.2016, p. 1–88;
43. Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and authentication services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Pub. OJ L 257, 28.8.2014, p. 73–114;
44. Recommendation (2002)2 of the Committee of Ministers to Member States on access to official documents - adopted by the Committee of Ministers on 21 February 2002 at the 784th meeting of the Ministerial Plenipotentiaries;
45. Recommendation R(2000)13 on European policy on access to archives - adopted by the Committee of Ministers on 13 July 2000;
46. Recommendation R(81)19 of the Committee of Ministers of the Council of Europe - adopted on 25 November 1981;
47. Recommendation R(94)13 of the Committee of Ministers of the Council of Europe;
48. Rules of Procedure of the State Commission on Information Security and its Administration, Pub. SG. no. 19 of February 28, 2017 (first and last revision);
49. Charter of Fundamental Rights of the European Union (2007/C 303/01), Pub. OJ C 202, 7.6.2016, p. 389-405.

George G. Dimitrov

LEGAL BASICS OF REGULATION OF THE INFORMATION IN BULGARIA

First PDF Edition

LAW AND INTERNET FOUNDATION
1303 Sofia, 54 Bulgarska Morava Str., fl. 6
Tel. +359 (2) 4460644
www.netlaw.bg, office@netlaw.bg

ISBN 978-619-7192-23-0

122