Law 7 May 2004 on experiments on human persons (Loi relative aux expérimentations sur la personne humaine).

Both the DPO and the Research Ethics Committees deal with legal and ethical compliance about data protection in research.

As regards the DPIA, the Belgian DPA has developed a blacklist and whitelist for data processing in need of DPIA.[58] However, to our best knowledge, there is no other specific tool for researchers to carry out DPIA or other data protection safeguards.

(iii) As regards the DPIA, the Belgian DPA has developed a blacklist and whitelist for data processing in need of DPIA.[59] However, to our best knowledge, there Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

As regards dual use, the General EU Council Regulation (EC) N. 428/2009 of 5th May 2009 about dual use is implemented by Articles 6 and 7 of the Flemish Government Decree of 14 March 2014 regulating export, transit and transfer of dual-use and the delivery of technical assistance (Belgian Official Gazette of 2 May 2014) and Articles 5 and 6 of the Walloon Government Decree of 6 February 2014 regulating export, transit and transfer of dual-use items and technology (Belgian Official Gazette of 19.2.2014)). These provisions require a special authorization for transit of listed dual-use items for military end use destinations.

As regards industrial espionage, researchers and innovators in Belgium can use the Belgian Act of 30 July 2018 on the Protection of Trade Secrets ('Act on Trade Secrets'). In addition, in most serious cases also Article 309 of the Penal Code (Code Pénal) can apply.

3 Bulgaria

Yordanka Ivanova (Sofia Bar Association/Sofia University)

[58] Authorité de protection des données, Liste des types d'opérations de traitement pour lesquelles une AIPD est requise, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste_des_traitements_AIPD.pdf

[59] Authorité de protection des données, Liste des types d'opérations de traitement pour lesquelles une AIPD est requise, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste_des_traitements_AIPD.pdf

3.1 Informed consent

3.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Personal Data Protection Act (last amended, SG No 17 of 26 Feb 2019)	https://www.cpdp.bg/en/index.php?p=element&aid=1194	Hard law	Transposes the Law Enforcement Directive 2016/680 and the derogations from the GDPR. The Act also regulates the status of the Commission for Personal Data Protection (CPDP), the remedies and the accreditation and certification in data processing.
Electronic Communications Act	https://www.mtitc.government.bg/sites/default/files/electronic_communications_act-en_kym_26022019.pdf	Hard-law	Transposes the e-Privacy Directive 2002/58/EC. Guarantees confidentiality of e-communications. Applicable to providers of public electronic communication services
E-Commerce Act	https://lex.bg/laws/ldoc/2135530547	Hard-law	Transposes the e-Commerce Directive 2000/31/EC – requires consent in relation to direct marketing messages to consumers. Applicable to all service providers sending unsolicited messages.
Health Act	https://www.lex.bg/laws/ldoc/2135489147	Hard-law	Regulates the processing and confidentiality of health and genetic data in the health sector and medical research.
Child Protection Act	https://www.mlsp.government.bg/index.php?section=POLICIESI&I=263&lang=_eng	Hard-law	Regulates the measures for protection of children (under 18) and the processing and

			disclosure of their personal data.
Act on Statistics	http://www.nsi.bg/en/content/218/basic-page/law-statistics	Hard-Law	Regulates processing of individual data collected and used for statistical purposes by the National Statistical Institute and the statistical authorities.
Guidelines from the CPDP in relation to consent	https://www.cpdp.bg/index.php?p=element&aid=1162	Soft-law	Clarifies the requirements for freely given, informed, unambiguous and affirmative consent, withdrawal of consent, consent given online, consent of children under 16 years old.
Guidelines from the CPDP when consent is not needed	https://www.cpdp.bg/index.php?p=element&aid=1159	Soft-law	Clarifies that consent for data processing is not needed in case of other legal grounds for processing (e.g. legal obligation, contract with the data subject, legitimate interests, public interest or official authority, transfer of obligations, photography in public places). It also enumerates a number of sectors where consent must not be sought – lawyers, health sector, postal and electronic services, banks etc.
Guidelines from the CPDP and the Electoral Commission for the processing of personal data in the course of elections	https://www.cpdp.bg/index.php?p=element_view&aid=1090	Soft-law	Clarifies who is data controller and processer in processing personal data in the course of elections and the legal basis for processing of general and sensitive data
Act on the Protection of Classified Information	https://www.lex.bg/laws/ldoc/2135448577	Hard-law	Regulates the generation, the processing, and the storing of classified

			information, and lays down the conditions and procedure for the release thereof and the access thereto.

Main regulatory tools addressing data protection issues and informed consent in Bulgaria

(i) The GDRP does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

No.

(ii) The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

In Bulgaria, the Data Protection Act is not applicable to national security issues. In this case, the processing of personal data should normally fall within the **Act on the Protection of Classified Information** which regulates the generation, the processing, and the storing of classified information, and lays down the conditions and procedure for the release thereof and the access thereto. "Classified information" is any information which is a State secret or an official secret, and any foreign classified information. State secret is defined as 'information, as listed in Schedule 1, the unauthorized access to which might threaten or prejudice such interests of the Republic of Bulgaria as relate to national security, defence, foreign policy or the protection of the constitutional order'. Official secret is defined as 'information generated or stored by government authorities or by the authorities of local self-government, that is not a State secret, and the unauthorised access to which might adversely affect the interests of the State or prejudice another interest protected by law'. The information subject of classification as an official secret shall be determined by law. The purpose of this Act is to protect classified information against unauthorized access and for this purpose it envisages very detail rules about the necessary measures for protection, including access management to classified information and the necessary background investigation procedures (articles 43-71), physical security (articles 72-79), document security (articles 80-82), personal security (article 83), cryptographic security (articles 84-88), security of communication and information systems (articles 89-94a), industrial security (articles 95-112), rules for disclosure or exchange with third state or international organisation (articles 113-116).

Article 34 also defines the periods of storage of classified information as follows:

1. of information marked as "Top Secret" - 30 years;
2. of information marked as "Secret" - 15 years;
3. of information marked as "Confidential" - 5 years;
4. of information classified as an official secret - 6 months.

Where national interest so requires, the State Information Security Commission may decide to extend these periods, provided however that the extension shall not exceed the original protection period. Upon the expiration of these periods, the classified information shall be declassified and the access to such information shall be governed by the Access to Public Information Act.

Quite importantly, the current governing coalition together with the State Agency for National Security has recently proposed a draft law (available at http://strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=4526) which makes possible the storage periods of classified information to be further prolonged:

1. of information marked as "Top Secret" - up to 90 years in total;

4. of information classified as an official secret - up to 2 years in total.

This proposal has not been voted yet by the National Parliament, but it has been seriously criticized by human rights organisations as it makes the state secret almost eternal, provides opportunity to classify a file with thousands of documents only because one single document is considered secret and also enables the Minister of Interior and the directors of secret services to destroy separately classified documents related to the operational-search activity of the services.

Name of Authority	Link	Is this an independent - body?	Number of employees	Level of activity (according to your appreciation)?	Response to requirements, questions, etc. made by the public
Commission for Personal Data Protection (CPDP)	https://www.cpdp.bg/en/index.php?p=rubric&aid=1	Yes	83	Moderate, mainly on request	Yes, app. within 20-30 days
Judicial Inspectorate - examines complaints of data subjects against courts in their judicial capacity and against the prosecution and the investigating authorities when personal data is processed for law enforcement purposes	http://www.inspectoratvss.bg/en	Yes	N/A	No evidence (newly established)	N/A

Information regarding Data Protection Authorities, Bulgaria.

(iv) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

There is no specific definition of 'research purposes' in the Bulgarian Data Protection Act. Research is however generally regulated by the Bulgarian Act for the Development of Research, which regulates the state policy in the field of research. Article 2 stipulates that in accordance with the National Strategy for Research, state-funded research should have proven relevance/importance and international recognition and should include research related to:

1. the creation of new research knowledge;

2. Bulgarian, history, language, culture and national identity;

3. promotion of the technology transfer and the development of the natural, technical, humanitarian and social sciences and innovations;

4. solutions to important problems in the field of economy, education, agriculture, environment, social processes, human resources, security, defence and health.

The research activity under this act should cover fundamental and applied research as well as the dissemination of the research outcomes. Fundamental research is defined as research, including experimentation or theoretical work undertaken with the main objective of gaining new knowledge for the fundamental reasons underlying events or facts under examination without any practical application or use of this knowledge.

As regards the priorities for state funded research, according to the National Strategy for research 2017-2030, the priorities for the fundamental research shall be linked to the current social challenges, including:

• competitiveness and productivity growth of the economy;

• social development, solutions to the demographic problem and poverty reduction;

• increasing quality of life – food, health, biodiversity, environment, city, transport etc.;

• energy and energy efficiency;

• cultural-historic heritage, national identity and development of culture of the society;

• national security and defence, reduction of damages caused by natural and man-made disasters.

The priorities for the applied scientific research are:

• current energy resources and energy efficient technologies;

• mechatronic and clean technologies;

• health and quality of life. Prevention, early diagnosis and therapy, green, blue and eco technologies, biotechnologies and eco-food;

• environment. ecology monitoring, raw material resources and bioresources, recycling and cleaning technologies;

• nano and quantum technologies;

• information and communication technologies;

• national identity and development. socio-economic development and governance.

(v) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

Only for medical research (see the answer to the next question), but not for general research. Article 25m of the Bulgarian Data Protection Act only states that personal data originally collected for a different purpose may be processed for the purposes of the National Archive Funds, for scientific, for historical research or for statistical purposes. In such cases, the controller shall apply appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject in accordance with Article 89 (1) GDPR.

(vi) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR? Which cases? Which safeguards?

In relation to safeguards for processing of sensitive data for research purposes, specific safeguards are envisaged for medical research regulated in detail in the Health Act. According to Article 28(1), point 6, health information may be disclosed to third parties for the needs of medical statistics or medical research only after the data identifying the patient have been deleted, i.e. anonymized.

Article 197 envisages that the Ministry of Health is responsible to organise and control the conduct of medical research on people. Medical research is defined as any experiment on people conducted with a view to increasing medical knowledge. Tested persons shall have all the rights of a patient. Medical research shall be conducted, while ensuring maximum safety for the health of the tested person and non-disclosing his/her personal data. The interests of the tested person shall prevail over the scientific and financial interests of the researcher at any stage of the medical research. Article 198 states that medical research on people shall not be conducted in any of the following cases:

1. it contravenes the law or medical ethics;

2. no evidence has been produced on their safety;

3. no evidence has been produced on the expected scientific benefits;

4. it does not correspond to the scientific objective and the medical research plan;

5. there is an increased risk for the health and life of the tested person.

No medical research on people shall be conducted with chemical substances and physical sources of radiation which may lead to changes of the human genome. No medical research on people shall be conducted with products of genetic engineering which may lead to the transmission of new properties of the progeny.

Article 199 provides that medical research shall be conducted only on persons who have given their informed consent in writing upon their notification in writing by the leader of the research on the essence, importance, scope and possible risks of the research. Consent with the participation in medical research shall be given only by a legally capable person understanding the essence, importance, scope and possible risks of the clinical tests. The consent shall be given in person and in writing. It may be withdrawn at any point of time.

Article 200 forbids carrying out of medical research on people who have been put under legal incapacity. Where no significant health benefits are expected, medical research shall not be conducted on pregnant women and breast-feeding mothers and prisoners.

Article 201 envisages that the medical research head shall be jointly liable with the other individuals on the research team for any material and non-material damage they have caused to the medical research participants as a result of effects suffered during the medical research. The medical research head shall take out insurance covering the liability of both the head and the other individuals on the research team for any material and non-material damage suffered by the medical research participants as a result of effects caused during the medical research. The general terms and conditions, the minimum insurance amount, the minimum insurance premium and the insurance procedure shall be set out in an ordinance issued by the Council of Ministers. Article 206 further envisages that the terms and conditions for the conduct of medical research shall be set out in an ordinance issued by the Minister of Health in consultation with the Minister of Education and Science. In this respect, in 2015 the Ministry of Health published for public consultation a draft Ordinance on the requirements for medical research, but this has not been adopted up to date (draft available at https://www.mh.government.bg/media/filer_public/2015/04/14/proekt-naredba-za-usloviata-i-reda-za-provezhdane-na-meditsinski-nauchni-izsledvania.pdf)

Article 202 further states that the leader of the medical research shall be a medical doctor or a doctor of dental medicine with recognised medical specialty and shall be responsible for the planning and conduct of the research. Medical research on people shall be conducted only by qualified specialists with higher education in the field of medicine, dental medicine, pharmacology, biology and biochemistry. Medical research may be conducted by foreign persons only on the basis of an agreement consulted with the Minister of Health.

Article 203 states that medical research shall be conducted upon obtaining a positive opinion from the local commission for ethics set up at the medical facility or research organisation conducting the medical research. The membership of the commission shall be determined by the head of the facility or organisation. Specialists involved in the preparation, organisation and conduct of the research may not sit on the commission. The local commission for ethics shall give its opinion within 30 days of receipt of the request by the leader of the research. The local commission for ethics shall supervise the conduct of medical research on people, on which it has given a positive opinion.

Article 204 envisages that upon the completion of the medical research on people, the leader of the research shall inform the local commission for ethics within 30 days. Under Article 205, the medical research may be terminated at any point of time in any of the following cases:

1. withdrawal of the consent of the tested person;

2. where hazardous impact on the health of the tested person has been found;

3. at the proposal of the leader of the research;

4. at the proposal of the chairperson of the local commission for ethics at the medical or healthcare facility in the event of proven violations in the course of its conduct.

Upon the termination of the medical research under Items 1 and 2, the leader of the research shall inform the local commission for ethics within 15 days. In the cases falling under Item 2, the medical research shall be terminated by order of the RHI director under the terms and conditions laid down in the ordinance provided for in Article 206.

Article 207 states that the Minister of Health shall determine, on an annual basis, research projects in the government research priorities in the field of medicine at the proposal of the rectors of higher schools, the directors of the national centres for public health affairs, heads

of research organisations and other legal entities and upon obtaining the opinion of the Supreme Medical Council.

Article 208 also envisages that the Minister of Health shall announce a competition to select contractors of research projects in the government research priorities. The terms and conditions for the conduct of competitions and the requirements to the applicants shall be set out in an ordinance issued by the Minister of Health in consultation with the Minister of Education and Science. Research projects shall be financed through government subsidies and other sources.

Article 208a envisages that the body of a deceased person may be used for educational and scientific research purposes in higher medical schools, once the death has been established as per the medical criteria and procedures laid down in the regulations under Article 18(1) of the Organ, Tissue and Cell Transplantation Act. Article 208b states that the body of a deceased person may be used for educational and scientific research purposes in higher medical schools, if the person is a Bulgarian national and had expressed explicit consent thereof while still alive. In the case of no consent, the body of a deceased person may be used for educational purposes in higher medical schools, upon obtaining, within a reasonably short time, the written consent of one of the following persons addressed in the same order as presented below:

1. spouse or cohabiting (common law) partner;

2. relatives in both the descending and ascending lines;

3. collaterals to the third degree of kinship;

4. relatives-in-law up to the second degree of kinship.

In the case of no consent of the diseased and no statutory consent due to the lack of the persons mentioned above, the body of a deceased person may also be used for educational and scientific research purposes. The procedures governing the use of bodies of deceased persons for educational and scientific research purposes in higher medical schools shall be laid down in regulations of the Minister of Health concerted with the Minister of Justice and the Minister of Interior.

Article 208c envisages that upon completing the post-mortem educational activities, the higher medical schools shall notify the relatives of the deceased person and shall pay the funeral costs. Higher medical schools shall arrange and pay the costs for the funeral of the deceased person in the following cases:

1. when consent has been given under Article 208b (1) and no persons within the meaning of Article 208b (2) have been found;

2. under the circumstances of Article 208b (3).

The more general question for the safeguards for processing of sensitive data for any purpose (not only research) is answered further down in the questionnaire.

(iii) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

There is no national or regional code of ethics in research. In principle, each university/research organisation has its own code of ethics, but these codes usually don't contain specific provisions for privacy/data protection except in the case of medical

research. Still, there is a general principle established under article 3 of the Act on the Development of Scientific Research that any scientific research needs to be ethical, transparent, public, accessible and applicable.

(iv) Does your national legislation give specific definitions of data processing for "statistical purposes"? Are there specific rules that apply to such data processing?

Yes, the Bulgarian Act on Statistics defines 'statistical purposes' as meaning "usage of the collected individual data for the development and production of statistical information, statistical analyses and prognoses". The same act defines the following principles in relation to the statistical activity: adequacy, accuracy, timeliness, punctuality, accessibility and clarity, comparability and logical connection. It also envisages that the collection of individual data is done on the basis of voluntary or obligatory participation of natural persons, households, economic entities or other organisations. The results from the statistical analysis included in the national statistical programme shall be available to the public.

Article 21 of the Act on Statistics envisages that natural persons are obliged to provide information only in relation to national census regulated by a separate law on the census. It also states that natural persons cannot be obliged to provide data in relation to their race, nationality, ethnic identity, religious beliefs, health, private life, political membership, criminal and administrative sanctions, philosophical and political beliefs. Article 22 further obliges the National Statistical Institute (NSI) to disclose in appropriate manner and inform in writing the persons who are subject to statistical research about their rights and obligations, the purpose, scope and means for carrying out the research as well as about the safeguards for confidentiality and protection of the classified information. Article 25 regulates that the individual data collected for statistical research represent statistical secret and can be used only for statistical purposes. Individual data received for the purposes of statistical research cannot be used as evidence in judicial or administrative proceedings. NSI and the statistical authorities and their staff may not disclose or provide: 1. individual statistical data; 2. statistical data which can be matched in a way that enables the identification of a specific statistical unit; 3. statistical information which aggregates data about less than three statistical units or about a population in which the relative share of the value of a surveyed parameter of a single unit exceeds 85 per cent of the total value of such parameter for all units in the population.

Article 26 envisages that individual data under article 25 can be disclosed only if transferred to 1) Eurostat if this is necessary for the development and production of European statistical information, or to 2) the National Statistical Institute by the statistic authorities if this is necessary for the development or production of the official statistical information. Individual data can be published only if the data subject has given his or her consent for this. Consent should be given in writing and it must clarify for which data the consent is given. The data subject should be able to withdraw his or her consent at any time in writing. The withdrawal of the consent shall not affect the lawfulness of the processing taken place so far.

Article 26a envisages that individual anonymous data can be disclosed with the permission of the NSI Director for the purposes of scientific research in universities or legal entities whose main activity is scientific research.

Article 27 obliges NSI and the statistical authorities to guarantee the protection of the individual data and prevent abuses by taking appropriate technical and organisational measures and providing access to such data only to staff who have signed a written declaration on oath to guarantee confidentiality of the statistical secret. The collection, processing, usage and storage of data that constitute statistical secret should be done according to an ordinance issued by the Director of the NSI. The statistical authorities are obliged to adopt internal rules for work with data that constitute statistical secret. The staff who are charged with the processing of data -statistical secret should sign a written declaration on oath to guarantee confidentiality of the statistical secret valid for 5 years after termination of their obligations. NSI and the statistical authorities are obliged to use the individual data only for statistical purposes except where data subjects have given written consent to allow use of the data for other purposes that must be concretely specified. The rules in relation to the statistical secret are obligatory for NSI and the statistical authorities in relation to all statistical research carried out under the Act on statistics. Registration, use, processing and storage of data that is classified information and represent state or official secret should be done in accordance with the Act for the protection of the classified information and the acts for its implementation. NSI is also obliged to maintain a register of the statistical units and Statistical register of the persons. The Information in these registers comes from the registers of the self-employed persons (BULSTAT), the commercial register, the National system for civil registration and other national registers and administrative sources, results from analyses carries out in accordance with the Act on Statistics and data provided in accordance with other national legislation.

Finally, with regard to the data subjects' rights, Article 25l of the Bulgarian Data Protection Act envisages that where personal data is processed for statistical purposes, Articles 15, 16, 18 and 21 GDPR shall not apply.

(v) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

Not in addition to the medical research examined above. In its non-binding guidance in relation to consent, the CPDP only repeats recital 33 of the GDPR that it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

3.1.2 Rights of data subjects and data processing

(i) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

No.

(ii) Are there any special requirements regarding informed consent at the national level?

No. There are just a number of sectoral legislative acts where consent is explicitly required for the disclosure/processing of certain categories of personal data such as:

- the e-Commerce Act – consent is needed for direct marketing/unsolicited commercial communication sent to consumers. Informed consent is also needed for storing information or gaining access to the consumer's device;

- the Child Protection Act - consent is needed for disclosure of children's data except where the data is disclosed to the competent authorities in order to take protective measures in relation to the child (see more on the question for children's data below)

- the Act on Statistics – consent is needed when personal data collected for statistical purposes will be used for other purposes or for the disclosure of individual's personal data to third parties (see more on the question above for statistical purposes)

- the Health Act – consent is needed for participation in medical research (as already explained above) and for disclose of health data except where the disclosure is specifically permitted in the Health Act (see more info in the questionnaire below)

- the Electronic Communications Act – consent is needed for the usage of the data for purposes other than the provision of the electronic communication services (e.g. research, marketing), for access to one's location data and for the disclosure of the data except the disclosure is specifically permitted in the act (see more info in the questionnaire below).

(iii) Are there any special requirements regarding data processing at the national level?

There are a number of additional/specific data processing activities regulated in the Bulgarian Data Protection Act (DPA):

- Article 25d states that a data controller or processor may **copy an identity document, a motor vehicle driving licence or a residence document** only if this is laid down in a law. This provision limits significantly the possibilities of controllers to copy these documents and is a particularity in comparison with other Member States.
- Article 25g states that **free public access to any information containing a personal identification number or a foreigner personal number** shall not be provided unless otherwise foreseen in law. Controllers providing services by electronic means shall take appropriate technical and organisational measures to ensure that the personal identification number or the foreigner personal number is not the only means of identifying the user when remote access to the service is provided. In order to provide administrative services by electronic means under the conditions of the Electronic Governance Act, the controller shall make it possible for the data subject to identify himself or herself following a procedure envisaged in law.
- Article 25h DPA states that the processing of personal data **for journalistic purposes and for the purposes of academic, artistic or literary expression** shall be lawful when carried out on the ground of freedom of expression and the right to information while simultaneously respecting privacy. In case of disclosure by transmission, dissemination or otherwise making available the personal data collected for these purposes, the balance between the freedom of expression and the right to information and the right of personal data protection shall be evaluated on the basis of the following criteria, if relevant:

1. nature of the personal data;

2. the impact that the disclosure of the personal data or the publishing of the data would have on the data subject's privacy and reputation;

3. the circumstances under which the personal data became known to the controller;

4. the character and nature of the statement under which the rights referred to in paragraph (1) are exercised;

5. the significance of the disclosure of personal data or the publishing of the data for the clarification of a matter of public interest;

6. taking into consideration whether the data subject occupies position under Article 6 of the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act or is a person who, because of his activity and public status enjoys lesser protection of his privacy, or whose actions impact the society;

7. taking into consideration whether the data subject has contributed with his actions for the disclosure of his personal data and/or of information about his private and family life;

8. the purpose, content, form and consequence of the statement when the rights pursuant paragraph (1) are exercised;

9. the compliance of the statement for exercising the rights paragraph (1) with the fundamental rights of citizens;

10. other circumstances relevant to the case.

When processing the data for journalistic and for the purposes of academic, artistic or literary expression, there are also a number of derogations from the GDPR provisions:

1. Articles 6, 9, 10, 30, 34 and Chapter V of Regulation (EU) 2016/679, as well as Article 25c, shall not apply;

2. the data controller or processor may deny the data subjects, fully or partially the exercise of the rights pursuant Articles 12 to 21 of Regulation (EU) 2016/679.

The exercise of the powers of the Commission pursuant to Article 58 (1) GDPR shall not affect the secrecy of information sources.

Where personal data are processed for the purposes of creating a photographic or audio-visual work by means of capturing the image of a person in the course of the public activity or in a public place, Article 6, Articles 12 to 21, and Articles 30 to 34 of Regulation (EU) 2016/679 shall not apply.

- Article 25j states that any data controller shall determine **a storage period for the personal data of candidates in staff selection procedures** which may not be longer than six months, unless the applicant has given consent for a longer period of storage. When the period of time expires, the employer shall erase or destroy the documents containing personal data unless otherwise provided for by a special law. Where in a staff selection procedure the employer or appointing authority has required the submission of originals or copies certified by a notary, ascertaining the physical and mental fitness of the applicant, the required qualification degree and experience for the position held, the employer or authority shall return the documents to the data subject who has not been approved for appointment within six months of the completion of the selection procedure unless otherwise provided for by a special law.

- Article 25k states that the processing of personal data for the **purposes of the National Archive Funds of the Republic of Bulgaria** shall be processing in the public interest. Articles 15, 16, 18, 19, 20 and 21 GDPR shall not apply in such cases
- Article 25n states that the processing of personal data for **humanitarian purposes** by public bodies or humanitarian organisations, as well as the processing in cases of disaster within the meaning of the Disaster Protection Act, shall be lawful. Articles 12 to 21 and Article 34 GDPR shall not apply in this case.

(iv) Are there any special requirements to exercise data subject's rights (right of access, correction, deletion of personal data)?

Article 37a DPA implements the **derogations from/restrictions of the data subjects' rights** envisaged in Article 23 GDPR. It envisages that the data controller or processor may deny the data subjects the exercise, wholly or partially, of the rights pursuant Articles 12 to 21 GDPR and may not perform the obligation pursuant Article 34 GDPR where the exercise of the rights or the performance of the obligation would result in a risk to:

1. national security;

2. defence;

3. public order and security;

4. the prevention, investigation, detection or prosecution of criminal offences or the enforcement of criminal penalties, including the safeguarding and the prevention of threats to public security;

5. other important objectives of general public interest, in particular an important economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

6. the safeguarding of judicial independence and judicial proceedings;

7. the prevention, investigation, detection and prosecution of breaches of codes of ethics for specifically regulated professions;

8. the protection of the data subject or the rights and freedoms of others;

9. the enforcement of civil law claims.

Paragraph 2 states that the conditions and procedure for the application of these derogations shall be established by law and in accordance with Article 23 (2) GDPR.

As far as the **procedure for the exercise of the data subjects' rights** is concerned, Article 37b DPA states that data subjects shall exercise their rights pursuant Articles 15 to 22 GDPR by submitting a written application to the data controller or by another method determined by the controller. Alternatively, a request may be submitted by electronic means under the conditions of the Electronic Document and Electronic Trust Services Act, Electronic Signature Act, the Electronic Governance Act and the Electronic Commerce Act. As a third option, a request may be submitted by accessing the user interface of the data processing information system after the person has identified himself or herself by the means of identification, relevant to the information system. According to Article 37c DPA, the request for the exercise of the rights must contain:

1. name, address, personal identification number or foreigner personal number or another similar identifier, of other data determined by the controller identifying the natural person, in relation to his/her activity;

2. description of the request;

3. preferred form in which information is to be received for the exercise of the rights;

4. signature, date of submission of the application and address for correspondence.

Where an application is submitted by an authorised person, the power of attorney shall be attached to the application.

Article 38 DPA further regulates the right to **complain to the supervisory authority – the Commission for Personal Data Protection**. The data subject shall have the right to bring the infringement of the GDPR before the Commission within six months after having become aware of the infringement but no later than two years after it. The Commission shall inform the complainant of the progress of the complaint or of the result within three months after the infringement has been brought to the attention of the Commission. The Commission shall issue a decision and may apply the measures referred to in points (a) to (h) and (j) of Article 58 (2) GDPR or in Items 3, 4 and 5 of Article 80 (1) and, in addition to or instead of them, the Commission may impose an administrative fine in accordance with Article 83 GDPR and under Chapter Nine of the DPA. Where the complaint is obviously unfounded or excessive, the Commission may adopt a decision to dismiss the complaint. The Commission shall send a copy of the decision to the data subject as well. In the cases referred to in Paragraph (1), where personal data is processed for the purposes referred to in Article 42 (1), the decision of the Commission shall contain only a finding about the lawfulness of the processing. The decision of the Commission can be appealed pursuant to the Administrative Procedure Code within 14 days of receipt. According to Article 38a DPA, the complaint to the Commission may be submitted by a letter, fax or by electronic means under the procedure of the Electronic Document and Electronic Trust Services Act. No action shall be taken on anonymous complaints and on complaints which are not signed by the complainant or by a legal or authorised representative.

Article 38b DPA states that by any infringement of the rights under GDPR and under this Act with the processing of personal data by the court when acting in the judicial capacity and by the prosecution and the investigating authorities when acting in the judicial capacity for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, the data subject shall have the right to submit **a complaint to the Judicial Inspectorate** within six months after becoming aware of the infringement but not later than two years after the infringement. In this case, Article 38a shall apply, mutatis mutandis. Article 38c. states that the complaint pursuant to Article 38b shall be examined by an inspector designated by the Inspector General on the basis of the random selection principle. Data relevant to the alleged infringement shall be collected when handling the complaint, including information from the data controller or processor. The complainant shall be informed of the progress of the complaint or of its result within three months after the infringement has been brought to the attention of the Inspectorate. Where the complaint is unfounded, the inspector shall give his or her decision which could be appealed pursuant to the Administrative Procedure Code within 14 days of reception of the decision. Where the complaint is founded, the

Inspectorate shall issue a decision on a proposal by the inspector. The decision could be appealed pursuant to the Administrative Procedure Code within 14 days of reception of the decision. Where the complaint is unfounded or excessive, the inspector may dismiss it.

According to Article 38d DPA, where an infringement of GDPR is ascertained in proceedings under Article 38c, depending on the nature and extent of the infringement, the measures referred to in points (a) to (g) and (j) of Article 58 (2) GDPR or in Items 3, 4 and 5 of Article 80 (1) shall be applied or administrative fines shall be imposed in accordance with Article 83 GDPR and under Chapter Nine of the DPA. The measures referred to in points (a) to (g) and (j) of Article 58 (2) GDPR and in Items 3, 4 and 5 of Article 80 (1) shall be applied by a decision of the Inspectorate on a proposal by the inspector who examined the complaint under Article 38b (1).

Article 39 DPA further regulates the **available judicial remedies.** Upon any infringement of the rights pursuant to GDPR and the DPA, the data subject may appeal against any actions or acts of the data controller and processor before the court pursuant to the Administrative Procedure Code. In the judicial proceedings, the data subject may claim compensation for the damage suffered as a result of an unlawful processing of personal data from the data controller or processor. The data subject may not bring a violation to the attention of the court if proceedings on the same infringement are pending before the Commission or a decision of the Commission regarding the same infringement has been appealed and there is no enforceable judgment of the court. At the request of the data subject, the Commission shall certify the lack of proceedings pending before it on the same dispute. The same requirement shall apply on any proceedings pending before the Inspectorate.

Article 40 DPA also ensures legal remedy against decisions implementing acts of the European Data Protection Board. Where the decision referred to in Article 38 DPA has been adopted to implement a binding decision of the EDPB, Articles 263 and 267 TFEU shall apply accordingly.

3.1.3 Minors, sensitive data and other additional categories of data processing

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

Data related to legal entities is not covered by the national data protection rules, but legal entities' trade secrets are protected in accordance with new Act on the Protection of Trade Secrets (SG No.28 from 5 April 2019) which transposes the Trade Secrets Directive 2016/943. Legal entities' legitimate interests are also respected in certain circumstances – e.g. right to opt out from unsolicited commercial communication (under the e-Commerce Act), confidentiality of their electronic communications (under the Electronic Communications act).

In relation to sensitive data, there are no other categories of sensitive data specified in the national rules in addition to those under article 9 GDPR. The following additional safeguards for the processing of sensitive data were found in the national legislation:

A. Health data is regulated in detail in the Health Act. Article 27 provides that the medical and health centres, doctors, dentists, pharmacists and other medical specialists with higher medical education, working in the national health system, can collect, process, use and

store health data. They are explicitly obliged to protect the health data collected and stored by them against unauthorized access. Article 27(3) envisages that the Minister of Health shall issue ordinances in consultation with the National Statistical Institute on the forms and content as well as the conditions and procedures for processing, usage and storage of health data and sharing of medico-statistical information. While there is an ordinance on the medico-statistical information collected and disclosed for statistical purposes, no other ordinance has been issued up to date on the general requirements for health data processing, storage and disclosure, so only GDPR remains applicable.

Article 28 of the Health Act further envisages that health information can be disclosed to third parties when:

1. the treatment of the person continues in another medical centre;
2. there is a threat to the health or life of other persons;
3. the information is necessary in order to identify a dead body or the reasons for the death;
4. the information is necessary for the needs of the state health control to prevent epidemies and spread-out of contagious diseases;
5. the information is necessary for the needs of medical expert activities and the social security scheme;
6. the information is necessary for the needs of medical statistics or medical research, having deleted the data identifying the patient;
7. the information is necessary for the needs of the Ministry of Health, the National Center on Health Information, the National Health-Insurance Fund, the regional heath inspectorates and the National Statistical Institute
8. the information is necessary for the purposes of an insurer licensed under the Bulgarian Insurance Code.

The disclosure of the health information under point 2 shall take place after the data subject has been informed about the intended disclosure.

Article 28b further envisages that the patient has the right to access to his or her health data, including copies of medical documents. The patient can also empower in writing another person to gain access to his or her health data as well as to make copies of the medical documents. In the event of death of a patient, his or her successors and direct relatives as well as indirect relatives up to forth kinship can have access to the health information of the diseased and make copies of his or her medical documents.

There is also an Ordinance on the conditions and procedures for occupational medicine (SG No. 14 from12.02.2008) which provides additional safeguards and regulates the processing of employees' personal data for the purposes of occupational health medicine.

The Health Insurance Act (articles 63-69) further regulate the information processed for the purposes of the activity of the National Health Insurance Fund (NHF), the purposes for which the data of the insured persons can be used and the organisations to which it can be disclosed as well as the right of insured persons to have access to their data. Recently, insured persons have been provided with online access to their NHF files containing information about the medical and dental health services used in the past 5 years through the following website https://pis.nhif.bg/main/pis-main_files/Rights_of_use.htm. The file can be accessed online through digital certificate

or unique access code which every insured person can obtain from the National Revenue Agency or the Regional Health Insurance Funds only in person (no possibility for empowerment of third persons or sending the request by post). In its privacy notice, NHF states that the connection between the server and the user's browser is SSL encrypted and all technical and organisational measures are taken in accordance with the data protection legislation to ensure data protection and confidentiality of the personal data. There is a disclaimer through in relation to the NHF's liability, stating that 'the information provided through the system is not an official document and it is possible that the provided information may be incomplete, inaccurate, containing errors or out-of-date due to reasons beyond the NHF's control'.

The Insurance Code also envisages certain safeguards when licensed insurance agencies process sensitive health data, including the obligation to ensure the data in their information systems are up-to-date, accurate, complete and reliable and to ensure the necessary conditions to guarantee its security (article 114), the obligation to keep insurance secrecy except disclosure is permitted in the code (article 149-150) and the prohibition of disclosure of any health information about the insured person to the person making the insurance when the insurer is different from the insured person (article 151).

B. Genetic data and its processing is regulated in detail in Section IV of the Health Act. Article 137 states that the protection of genetic health shall be ensured through health activities aimed at: 1. preventive and diagnostic tests to prove and classify genetic diseases; 2. dispensary registration of persons with higher risk of occurrence and development of genetic diseases; 3. treatment of hereditary diseases, innate anomalies and predispositions; 4. identification of hereditary signs and identification of a parent; 5. preservation of genetic information. Article 138 regulates the preventive genetic tests, while Article 139 focuses on the genetic tests before childbirth in particular. According to Article 141 genetic tests and the taking of biological material for genetic tests for medical or research purposes shall be carried out only upon receipt of the informed consent of the tested persons given in writing and in case of children, persons with mental disorders and persons under legal incapacity at the permission of the commission for medical ethics at the respective medical facility. The results of genetic tests and screening may not be used for discrimination against the tested persons. Para. 4 states that the information about the human genome of persons shall constitute personal data and may not be disclosed to employers, health insurance organisations and insurance companies. Under Article 142, genetic tests for medical or research purposes shall be carried out by accredited genetic or independent laboratories. The Minister of Health shall issue an order on the National Genetic Laboratory responsible to provide methodological guidance and supervision of the activities of genetic laboratories and maintain a national genetic register. Article 143 obliges the accredited genetic and independent laboratories to inform the National Genetic Laboratory on a monthly basis of the genetic tests performed and the results thereof and establish and maintain an administrative register of the tests they have performed. Article 144 states that the genetic laboratories at medical treatment facilities may set up DNA banks for removal and preservation genetic material for research and medical purposes. They shall register their DNA banks with the Ministry of Health within seven days. Article 144a envisages the creation of a national register of rare disease patients for the purposes of establishing the type and frequency of rare diseases and for the purposes of planning and providing rare disease-related preventive, diagnostic and therapeutic activities. The terms and procedures for recording rare diseases shall be set out in regulations issued by the Minister of Health.

C. Political beliefs – The Bulgarian Electoral Code provides safeguards to ensure secrecy of vote in the course of European, national, presidential and municipal elections. Article 180 prohibits any demonstration/disclosure by a voter to the public or to the electoral commission of how he or she has voted before casting the bulletin in the polls. Article 181 also forbids the usage of mobile devices, cameras and other technologies with a view to filming or shooting the vote. In case of violation of these prohibitions, the bulletin shall be annulled by the electoral commission and the voter shall not be allowed to cast a second vote. Article 183 also forbids other persons to approach the voting cabin within less than 3 meters when there is a voter inside. Article 202 establishes the principles that the vote shall be personal and secret. The CPDP and the Central Electoral Commission have also issued joint guidelines for the European elections 2019 in relation to the processing of personal data. The guidelines specify that political parties, coalitions, members of Initiative Committees, electoral commissions and other public authorities are controllers in respect of the processing of personal data of voters/citizens. Data Processors could be sociological agencies or marketing companies acting under the instructions of a political party that carry out targeting research or political campaign in relation to identified voters. The legal grounds for processing can be legal obligations (e.g. the Electoral Code) or consent (e.g. when collecting signatures for the registration of a party/coalition for elections, carrying out sociological researches or sending targeted unsolicited messages with the purpose of political campaign). Regarding the processing of political beliefs as sensitive data, the guidelines point to article 9(1)d) GDPR which allows parties to process data about the political beliefs if that processing relates solely to their members or to former members or to persons who have regular contact with the party in connection with its purposes and provided that the personal data are not disclosed outside without the consent of the data subjects. This provision however is deemed inapplicable in cases where the political party processes the data of potential members, partisans or voters as the CPDP considers that in this case there is no clear connection with the political entity. In the course of elections, the main legal ground is considered instead Article 9(1)(g) GDPR substantial public interest, on the basis of Union or Member State law (e.g. Constitution, Electoral Code) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Other possible grounds are data subject's consent or data manifestly made public by the data subject (article 9(1) a) or e) GDPR).

D. Religious beliefs - Article 13 of the Act on Religious Beliefs establishes secrecy of confession. No other safeguards were found in relation to the processing of data about one's religious beliefs.

As far as other categories of data are concerned (non-sensitive), a specific category very well regulated at national level are data and meta-data processed in relation to the provision of public electronic communication services regulated by the Act on Electronic Communications (transposing the e-Privacy Directive 2002/58/EC). Confidentiality and protection of personal data are regulated in great detail in articles 245-262. Article 245 obliges the undertakings providing public electronic communications networks and/or services and their employees not to disclose and disseminate the communications and the related traffic data, location data, as well as the data necessary to identify the user, which have come to the knowledge of the said undertakings in the course of provision of electronic communications networks and/or services. Article 246 states that for the purpose of protecting the confidentiality of communications and the related traffic data, the listening, recording, storage or other kinds of interception or surveillance of

communications by others than the sender and recipient of the communication without the express consent of the sender and recipient shall be prohibited, with the exception of the cases where this is provided for in a law. Exceptions to this general prohibition are envisaged in para. 2 and article 247.

Article 248 further specifies the categories of personal data of users that can be used directly for the provision of electronic communications services, including the types of traffic data, data necessary for the formation and reliability of subscriber bills and location data. Article 249 also forbids undertakings to request other data for provision of services, unless otherwise provided for by law or where the service cannot be provided without requiring other data. The undertakings may not make the provision of the services contingent on the consent of the user that the data thereon be used for other purposes. The collected personal data of users who are natural persons shall be processed in accordance with this Act, and for matters not laid down in this Act shall refer to the provisions of GDPR.

Article 250 regulates in great detail the traffic data of users and the purposes for which traffic data can be used by the undertakings. A number of provisions (articles 250a to 250f and Article 251, 251a, allowing indiscriminate storage and access to traffic data by intelligent service and law enforcement agencies) have been declared unconstitutional by the Constitutional Court of the Republic of Bulgaria - SG No. 23/2015 in line with the landmark Digital Rights Ireland judgement of the CJEU. These provisions have been supplemented by:

- Articles 251b sets the storage period of data of 6 months, unless the data need to be retained for detection and investigation of serious criminal offences. The types of data to be destroyed under this obligation are further specified in Article 251i. Article 251g obliges the undertaking to destroy the data after the expiration of the time-limit under article 251b and provide CPDP with a record of the data destroyed each month.

- Article 251c regulates the access to the data for law enforcement, national security purposes, anti-corruption, civil protection and other legitimate purposes and the requirements and content of the requests for disclosure.

- Article 251d requires permission by the chairperson of the district court or by a judge authorized thereby at the whereabouts of the seat of the body that requested access, for which an order for provision of access to the data shall be issued.

- Article 251d.1 provides exception in cases of imminent danger of certain crimes where immediate access to the data must be provided. The data provided shall be destroyed immediately by the authorities, if the court issues a refusal within 24 hours, of which the undertaking providing public electronic communication networks and/or services shall be immediately informed. Otherwise, the actions already carried out shall be validated with the order of the court.

- Article 251e obliges the undertakings to ensure 24-hours-a-day, 7-days-a-week opportunity for receiving the orders for Access. Article 251f further regulates the maintenance of a register and the responses to such requests.

- Article 252 clarifies the functions of the staff within the undertaking that are allowed to process traffic data.

- Articles 253-6 regulates the processing of location data, imposing obligations for prior consent of the data subject, disclosure and access to the data and some additional requirements.

- Article 257 regulates the "tone dialling", "calling line identification" and "connected line identification" functions

- Articles 258-9 regulates the telephone directories in a printed or electronic form and the access to them by end-users

- Article 260- 260a regulates the itemized bills and the other detailed information about the services used

- Article 261 regulates the use of the data of consumers for marketing purposes which need prior consent unless used for the dispatch of similar products or services and if the consumer is given a right to object. Some additional requirements are also envisaged (e.g. clear identity of the sender etc.)

- Article 261a states that CPDP is the supervisory authority responsible for the activity of the undertakings providing public electronic communications networks and/or services and clarifies their obligations to ensure the protection and security of the processed data. (see more in the questions on security below)

- Article 261b further empowers the National Assembly, acting through a committee to exercise parliamentary oversight and monitoring of the procedures for permission and implementation of access to the data.

- Article 261c to 261e further regulate the response to and reporting of data breaches (see more in the questionnaire on security).

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

The Child Protection Act envisages that children's rights cannot be restricted or privileged on the basis of race, nationality, ethnicity, sex, origin, economic status, religion, education, beliefs or disability. Article 11a envisages that information and data in relation to children cannot be disclosed without the consent of their parents or legal representatives except where the information is that the child is in need of protection and this information is disclosed to Direction "Social care", the State Agency for Child Protection or the Ministry of Interior. In cases where a measure for protection is taken with regard to a child, it is forbidden to disclose information and data in relation to that child without the written opinion of the authority for child protection that has taken the measure. When the child is aged 14 and above, he or she should give consent for the disclosure of the data.

Article 16 envisages that all information obtained in administrative or judicial proceedings that affect children cannot be disclosed without the consent of the parents or the legal representatives and if the child is aged 10 or above without his or her consent. The Court may allow the public authorities responsible for the child protection to use such information without the consent of the parents and the child if this is necessary for the best interests of the child and for taking measures for his or her protection. Social workers and public servants are obliged to comply with the legal obligations for the protection of the personal data obtained during or in relation to the implementation of the measures for the protection of the child as well as to respect the dignity of the child.

According to Article 25c of the Data Protection Act, in relation to the information society services consent of minor is valid if the child is aged 14 or above.

system of disabled persons in accordance with the Act on the Electronic Identification.

(iii) Are there other vulnerable individuals identified in your national legislation?

There is also an Act on the Protection of Persons with Disabilities, but it contains only a general obligation to collect and use the personal data of persons with disabilities in accordance with the requirements of the applicable data protection legislation. People with disabilities should have access to their profiles in the centralized

3.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country? ´

Article 25f DPA stipulates that a data controller or processor may process personal data of deceased persons only if there is a legal basis for this. In such cases, the data controller or processor shall take the appropriate measures so that the rights and freedoms of others or a public interest would not be adversely affected. Upon request, the controller shall provide access to personal data of a deceased person, including by providing a copy, to the heirs of the person or to other persons with a legitimate interest.

3.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

There are no general requirements in relation to accountability, but specific additional accountability obligations are envisaged in the Data Protection Act with regard to large scale systematic monitoring of publicly accessible areas and the accountability of employers.

Article 25e states that data controllers and processors shall adopt and apply rules for large scale personal data processing or for a large-scale systematic monitoring of publicly accessible areas, including video surveillance, if the controller or processor implements appropriate technical and organisational measures for safeguarding the rights and freedoms of data subjects. The rules on large scale systematic monitoring of publicly accessible areas shall state the legal grounds for setting up a monitoring system, its scope and means, storage period of the information records and their erasure, the individuals' right of access, the provision of information to the public about the monitoring, as well as restrictions with regard to the access of third parties. For this purpose, the CPDP shall issue guidelines to data controllers and shall publish them on its Internet site.

Article 25i states that any employer or appointing authority, in the capacity of data controller, shall adopt rules and procedures for:

1. use of an infringements reporting system;

2. restrictions on the use of internal company resources;

3. implementation of control system for access, working time and discipline.

The rules and procedures referred above shall contain information relating to the scope, obligations and methods for its practical application. These shall take into consideration the activity of the employer or appointing authority and the related nature of work and may not restrict the rights of data subjects pursuant to GDPR and pursuant the Data Protection Act. Employees and workers shall be informed about these rules and procedures.

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

The Data Protection Act does not envisage any additional requirements for Data Protection Impact Assessment (DPIA). However, additional circumstances where DPIA must be done are envisaged in a list prepared by the CPDP and approved by the EDPB in accordance with the consistency procedure. This list requires DPIA in Bulgaria also in case of:

- large scale processing of biometric data with the objective of identification that is not sporadic;

- processing of genetic data with the objective of profiling which produces legal or similarly significant effects on the data subject;

- processing of location data with the objective of profiling that produces legal or similarly significant effects on the data subject;

- where the provision of information under article 14 GDPR proves impossible or would involve a disproportionate effort or in so far as the provision of this information is likely to render impossible or seriously impair the achievement of the objectives of that processing when the processing is of large-scale data;

- processing of data carried by a controller whose main establishment is outside the EU when its appointed legal representative is based on the territory of Republic of Bulgaria;

- regular and systematic processing where the provision of information under article 19 GDPR proves impossible or would involve a disproportionate effort;

- processing of data of children in the provision of information society services;

- migration from existing to new technologies when this is linked to large scale processing of data.

3.2 Commercialization of data

3.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Act on Obligations and Contracts	https://www.lex.bg/laws/ldoc/2121934337	Hard-law	Regulates the lawfulness and validity of contracts and other general issues under civil and obligation law (e.g. types of contracts, contractual liability, torts etc.)
Act on The Protection of Trade Secrets	https://www.lex.bg/bg/laws/ldoc/2137192307	Hard-law	Regulates the protection of trade secrets of legal and natural persons and the exceptions to them. Transposes the Trade Secret Directive 2016/943

Act on the Copyright and Neighbouring Rights Protection	https://lex.bg/laws/ldoc/2133094401	Hard-law	Regulates the protection of copyright and neighbouring rights
Act on Access to Public Information	https://lex.bg/laws/ldoc/2134929408	Hard-law	Regulates the access to public information and the re-use of public sector information. Transposes Directive (EU) Directive 2003/98/EC
Act on the Access to Spatial Information	https://www.lex.bg/laws/ldoc/2135667082	Hard-law	Regulates the establishment, maintenance and use of the infrastructure for spatial information, securing access to spatial data and rendering services related to data in the field of the environment or to activities which may have an impact on the environment by ensuring compatibility and safety in cases of data sharing. Transposes the Inspire Directive 2007/2/EC

Main regulatory tools addressing data commercialization in Bulgaria.

3.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

Yes, in Bulgaria the principle of contractual freedom allows contracts to be concluded, if not contravening the mandatory provisions of the law and good morals (Article 9 of the Obligations and Contract Act). We don't have an explicit legal prohibition of entering into contracts in exchange of personal data and the Bulgarian courts have not yet proclaimed such practices as contravening the good morals. In line with the e-Commerce Directive, Article 18 of the Bulgarian e-Commerce Act also clarifies that its obligations are applicable to providers of free information society services. In addition, the Consumer Protection Act applies to consumer contracts for the provision of good and services against remuneration, but also to contracts for digital content, which is not supplied on a tangible medium, that may be free and provided in exchange of personal data. Some contractual provisions or data harvesting practices for collection of personal may be, however, consider aggressive or presenting unfair contractual terms, so it is still possible to find them illegal under the applicable consumer protection law.

(ii) Do you know if these practices are routinely performed?

Yes, mostly in the digital space where services are provided for free

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

The only requirements for renumeration of data subjects if profit is made out of their personal data, that I am aware of, are in cases where the personal data constitute at the same time objects protected by copyright and neighbouring rights (artistic, literary, scientific and other protected works of personally identifiable authors). The holder of the copyright could claim compensation based on contracts on use (articles 35-38) or where free use of his or her works is permitted by law without permission but with the obligation to pay compensation (regulated under article 25 and 26 of the Act on copyright and neighbouring rights). Performing artists also have a right to compensation as part of their economic rights regulated by articles 74-84 of the same act.

One particular case where a data subject could possibly claim a remuneration of the further use of their data is portrait (photography or fine art) of a person different from the author regulated under Article 13 of the Copyright Act. In this case the copyright of the portrait shall belong to the author, but he or she may negotiate with the person who appears on the portrait the terms of the use of such works. The depicted person must give his or her consent for its creation unless:

1. the portrait was made in the course of the public activity of the depicted person or in a public place;

2. the portrait is only a detail in a work of art depicting a meeting, procession or landscape;

3. the depicted person received a fee to pose, unless agreed otherwise between the author and the depicted person

(iv) Do you have any particular national regulation on the secondary use of data?

The re-use of personal data for statistical and research purposes was already examined in part I of the questionnaire. In addition, the secondary use of objects protected by copyright and neighbouring rights are regulated by the Act on copyright and neighbouring rights. In principle, the use of protected works can be only done with the consent of the holder of the right and on the basis of a contract for use (article 35-37). Article 36 states that by concluding a contract on the use of his work, the author shall grant the user exclusive or non-exclusive rights to use the said work on specific terms and for compensation. The granting of exclusive rights shall be explicit and in writing. Whenever no such provision exists, it shall be considered that non-exclusive rights have been granted. If no term has been specified in the contract, it shall be assumed that the right to use a work has been granted for a period of three years, or five years for architectural designs. If the contract does not specify a territory on which a user may use a work, the country of which the user is a national or the country of his seat, if he is a legal person, shall be considered as such territory. The contract shall be concluded individually, by a collective management organisation or through an independent management entity. Article 37 states that a contract under which an author has granted use of all works which he may create for the rest of his life shall be considered null and void. A contract on the use of a work may not be concluded for a term exceeding ten years. Whenever such a contract has been concluded with a longer term of validity, it shall remain in force for ten years only. This limitation shall not apply to contracts for architectural designs. Article 38 regulates the compensation of the author under a contract for any manner of use of his works which may be defined as a portion of the revenues resulting from the use of his work, as a fixed one-time amount or in other forms. Whenever the one-time compensation proves obviously incommensurate with the revenues resulting from the use of his work, the author may claim an increase of the said compensation. If no agreement can be reached between the parties, the issue shall be resolved through the court's ex aque et bono.

There are also certain exceptions provided for in the law where free use of protected works could be done without a contract and without the consent of the rightsholder. In particular, Article 24 allows free use without permission from the author and no compensation in the case of:

1. temporary use of works if it is transitional and incidental by nature, is of no independent economic significance, constitutes an inalienable and important part of the technical process, and is conducted for the sole purpose of allowing: a) transfer via network through an intermediary; or b) other allowed use of a work.

2. the use of quotations from already announced works for critical appraisals or reviews by providing due indication of the source and name of the author, unless that is impossible to do; Quotations shall be made in the customary manner and their volume shall be justified by their purpose;

3. the use of parts of published works or of a moderate number of small works in other works in a volume that is required for the purposes of preparing an analysis, commentary, or other scientific research; such use shall be admissible only if it is done for scientific or educational purposes and if reference is made to the source and name of the author, if this is not impossible;

4. the use as current news in the press and other media of addresses, reports, sermons, and others or parts thereof delivered at public gatherings, as well as speeches delivered in the course of legal proceedings, if reference is made to the source and name of the author, if this is not impossible;

5. use by the mass media of articles on current economic, political, and religious topics in all cases where such reproduction is not expressly forbidden if reference is made to the source and name of the author, if this is not impossible

6. reproduction by photographic, cinematographic or similar manner, as well as audio or video recordings of works related to a current event for the use of such works by the media in a limited volume for the purpose of providing news coverage if reference is made to the source and name of the author, if this is not impossible;

7. use of works that are on permanent display in streets, squares, and other public places without mechanical contact copying, as well as their broadcast by wireless technology or cable broadcast or by other technical means, if such broadcast is carried out for informational or other non-commercial purpose;

8. the public presentation or performance of published works in educational institutions if this does not involve the collection of revenues from such performance and if the participants in the preparatory work and the actual public performance do not receive compensation;

9. reproduction of already published works by generally accessible libraries, research and educational institutions, museums, and archives for educational purposes or to ensure the preservation of the work inasmuch as such action is not undertaken for profit;

10. the use of previously released works for the benefit of people with disabilities if it is directly related to the particular disability and is not for profit, except for the cases referred to in Section II of this Chapter;

11. providing access to natural persons to works that belong to collections of organizations as described in item 9 if this is not done for commercial purposes and not for profit;

12. temporary copying of works by radio and television organizations, to which the author has granted the right to use his work and broadcast it by their own technical means and for the purposes of their own broadcasts within the scope of the permission granted; copies that are of important documentary value may be kept in official archives;

13. use of works for the purposes of national security, in judicial or administrative proceedings, and in parliamentary practice;

14. use of works in religious ceremonies or official ceremonies organized by public authorities;

15. use of buildings that are considered works of architecture or of plans thereof for the purpose of the reconstruction of such buildings, performed after consultation with the relevant organisation for collective management of rights.

These provisions shall not apply to computer applications that are regulated by articles 70 and 71.

Article 25 further regulates the free use of works without consent of the holder of the copyright, but with obligation to pay compensation:

1. to reproduce for non-commercial purposes printed works, with the exception of musical note material, on paper or other similar media through photocopying or other similar method that yields similar results;

2. reproduction of works regardless of the media by natural persons for their personal use if such reproduction is not done for commercial purposes.

The provision in item 2 shall not apply to computer software and architectural designs. Computer software is explicitly regulated in a different way in article 70 and 71. The Compensation for Free Use of copyright protected works is further regulated in article 26.

Specific regulation for use of protected works is further envisaged for publishing contracts (articles 43-54), contracts on public presentation and performance (articles 55-58), contract for publishing in a periodical (articles 59-61), making and using films and other audio-visual material (articles 62-67), use of works of fine art, architecture and photography (articles 68-69), use of computer software (articles 70-71), special rules on the use of orphan works and sound recordings (articles 71b-h).

Another Bulgarian act regulating secondary use of data is the Act on Access to Public Information which regulates the right of access to public information, as well as to the re-use of public sector information. "Public information" is defined as any information pertaining to public life in the Republic of Bulgaria and enabling members of the public to form their own opinion regarding the operation of the entities obligated under the law. "Public sector information" is defined as any information materialized on a physical medium, stored inter alia as a document, sound or visual recording, and collected or created by a public sector body. Article 2a states that "Re-use" of public sector information shall be the use of such information for commercial or non-commercial purposes other than the initial purpose for which the said information was created within the powers or functions of a public sector organization. Article 4 defines as holders of the right to access to public information and re-use of public sector information any Bulgarian citizen, foreigner and stateless person in Bulgaria as well as any legal person. The procedure for re-use of public sector information is regulated in particular in articles 41a to 41j. Article 41a states that public sector information shall be provided in the format

and in the language in which it was collected, resp. created, as the case may be, or in another format at the discretion of the public sector body, as well as in an open, machine-readable format, together with the relevant metadata. The format of metadata in such cases shall conform to the official open standards. Public sector bodies shall not be obligated to provide information for re-use where this requires the creation or adaptation of such information or where this involves the provision of extracts from documents or other materials where this would involve a disproportionately large effort that goes beyond the limits of a routine operation. Upon request by the applicant and where possible, the information requested shall be made available through electronic means at the supplied electronic address or in other appropriate manners for provision of the information in electronic form. There is also an ordinance (SG No. 48 from 24 June 2016) on the standard terms and conditions for re-use of public sector information and for the publication of public sector information in open format for commercial or non-commercial use. Information constituting a piece of intellectual property which libraries, including ones of schools of higher learning, museums and archives, are authorised to use, shall be provided for re-use solely subject to an authorisation by the owner of the intellectual rights thereupon. The re-use of information from documents archived at the National Archive shall take place subject to the terms, conditions and procedure as per Chapter Six of the National Archive Stock Act and in compliance with this Act.

Article 41b further regulates public sector information which is not provided for re-use, including:

1. whereof the content is related to activities falling outside the scope of the powers and functions of public sector bodies as determined by a law, rules of organisation or statutes and/or an act whereby a public procurement contract is awarded;

2. where to a third party holds an intellectual property right;

3. which has been collected or created by public-service radio and television broadcasters or regional centres thereof;

4. which is the property of schools, higher learning establishments (except the libraries thereof), scientific research bodies, including ones created for the dissemination of the products of scientific research, and of cultural organisations, with the exception of libraries, museums or archives;

5. constituting classified information;

6. containing a statistical secret collected or stored by the National Statistical Institute or another statistical body;

7. containing an industrial or trade secret or a professional secret within the meaning of a law;

8.for the obtainment of which the applicant must prove their legal interest in accordance with a law;

9. constituting parts of documents that only contain emblems, coats pf arms or insignia;

10. containing personal data the re-use of which would constitute inadmissible access to, or inadmissible processing of, personal data subject to the requirements for their protection.

In these cases, only that part of the information access to which is not restricted shall be provided for re-use. In case of an overriding public interest, the public sector body shall provide for re-use information containing industrial or trade secrets, but the public sector

body may forbid the re-use of such information for commercial purposes or in a manner as would lead to unfair competition or otherwise restrict competition within the meaning as per Section Two of the Protection of Competition Act. Article 41i states that the existence of personal data in the public sector information which is requested for re-use may not be grounds for refusal in the cases where the said information constitutes or is part of a publicly accessible register. Article 41f further regulates the procedure for Provision of Public Sector Information for Re-use, including the requests and the obligation of the recipient of the information to pay fees in circumstances.

(v) Do you have any specific protection for metadata or non-personal data in your country?

In principle, non-personal data can be protected as part of a data-base under the Copyright Act (already examined above) or as trade secrets protected by the recently adopted Act on the Protection of Trade Secrets. Article 3 defines 'Trade secret' as any commercial information, know-how and technological information which meets all of the following requirements:

1. it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

2. it has commercial value because it is secret;

3. it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Article 4 states that trade secret holders are any natural or legal person lawfully controlling a trade secret. The Trade Secret Act transposes the Trade Secret Directive 2016/943 - if necessary for the research project, its provisions could be further analysed.

There is also an Act on the Access to Spatial Information which regulates the establishment, maintenance and use of the infrastructure for spatial information, securing access to spatial data and rendering services related to data in the field of the environment or to activities which may have an impact on the environment by ensuring compatibility and safety in cases of data sharing. Article 1 states that the infrastructure for spatial information includes metadata, spatial data sets and spatial data services, network services and technology; agreements on sharing, access and usage; coordination and surveillance mechanisms; processes and procedures introduced, managed or performed under this act by 1. public authorities that, by virtue of a statutory instrument, collect, establish, keep and distribute updated spatial databases with regard to the exercise of their powers and render public services related to them, and 2. third parties, other than the parties referred to in point 1, may provide spatial data created and kept by them, as well as related services, within the infrastructure for spatial information. The Act on the Access to Spatial Information transposes the Inspire Directive 2007/2/EC - if necessary for the research project, its provisions could be further analysed.

3.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

Data is not specifically classified under Bulgarian law as a product/commodity/good or service. "Data" is in principle mentioned in numerous sectoral laws, but there is no strict definition of its nature except for the definition of 'personal data' as defined in the GDPR

and 'public information/ public sector information' as defined in the Act on the Access to Public Information examined above.

The Bulgarian law defines 'good' as 'a tangible movable item, with the exception of items sold by way of execution or otherwise by authority of law, as well as items abandoned or forfeited to the Exchequer and put up for sale by State bodies. Water, gas and electricity, where they are put up for sale in a limited volume or a set quantity, shall also be goods. Therefore, I find it possible under Bulgarian law to construe data as a 'good' when it is materialized in a movable item and is put on sale (periodicals, DVDs etc.). By contrast, service is defined as 'any physical or intellectual activity which is performed independently, is intended for another person, and whose principal object is not the transfer of possession of a thing'. Thus, the provision, consultation, aggregation, analysis of certain information could be in my opinion characterized as a 'service'. In the public domain in Bulgaria the provision of official documents and public sector information is also defined as a 'service'. The definitions of goods and services mentioned above are taken from the Bulgarian Consumer Protection Act, which transposes the Consumer Rights Directive 2011/83/EU, so these should normally have the same meaning in all Member States. In distinguishing whether data must be conceived as a good or service it may be relevant to assess the purpose of the contract whether it aims to transfer ownership or not and in mix contracts what is the main purpose as suggested by the CJEU case-law cited in the Commission's guidance on the application of the Directive 2011/83 https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0_updated_0.pdf. It is interesting also that the Directive defines as a third separate type 'contracts for supply of digital content' where the data is not materialized in a movable item - see p. 5.

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

According to Article 4, item 4 of the Copyright Act, data shall not be object to copyright protection, so in Bulgaria data as such cannot benefit from copyright protection. Article 11 of the same act establishes a copyright over collections, anthologies, bibliographies, data-bases and other similar materials that shall belong to the person who has collected or arranged the works and/or material contained therein, unless agreed upon otherwise in a contract. The rights of the producers and legal users of data-bases are further regulated in Articles 93b – h. If necessary for the project, these provisions could be further analysed.

In addition to data-bases, data could be also protected as trade secrets as provided for by the recently adopted Act on the Protection of Trade Secrets which transposes the Trade Secret Directive 2016/943 – if necessary for the projects, its provisions could be further analysed.

I am not aware of specific mechanisms to determine the value of the data except in cases of compensation for use of works protected by copyright and other neighbouring rights and in case of re-use of public sector information when the recipients of the public sector data need to pay fees for obtaining this information.

3.3 Security and cybersecurity

3.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Cybersecurity Act (SG No.94 from 1 Nov 2018)	https://www.lex.bg/bg/laws/ldoc/2137188253	Hard-law	Transposes the NIS Directive. Applicable to 1. Administrative authorities, 2. providers of digital services and operators of essential services in one of the following sectors: energy, transport, banking, financial market infrastructure, healthcare, potable water supply and delivery or digital infrastructure. 3. persons carrying out public functions when providing admin services electronically; 4. organisations, providing public services when providing admin services electronically.
Ordinance on the minimal level of network and information security (SG No. 59 from 26 July 2019)	https://www.lex.bg/en/laws/ldoc/2137195046	Hard-law	Transposes the NIS Directive. Envisages minimal technical, organisational and technological measures in relation to: 1. Governance of Network and Information Security, 2. Protection, 3. Continuity and 4. Control.
Electronic Communications Act	https://lex.bg/laws/ldoc/2135553187	Hard-law	Transposes the e-Privacy Directive 2002/58/EC. Obliges providers of public electronic networks and/or services to ensure integrity, security and business continuity of the networks and to guarantee protection against unauthorize access to personal data by taking appropriate technical and organisational measures in accordance with the risks.
Ordinance № 1 from 21 December 2016 on notification of	https://www.cpdp.bg/?p=element&aid=1048	Hard-law	Clarifies the circumstances where the undertakings providing public electronic communication networks and/or services shall notify users about personal data breaches, the form and means of the notification

personal data breaches in public electronic services			
Act on Payment Services and Payment Systems	http://bnb.bg/bnbweb/groups/public/documents/bnb_law/laws_payment_services_en.pdf	Hard-law	Transposes the PSD2 - Directive 2015/2366. Obliges payment services providers to establish appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide, and establish and maintain effective incident management procedures
Ordinance of the CPDP on the minimal level of technical and organisational measures and permissible data processing (repealed as of 25 May 2018)	https://www.cpdp.bg/userfiles/file/Archive/Archive_Ordinance_1_30_01_2013_En.pdf	Expected to be transformed in soft-law/guidance	Envisages different types of protection, including physical, personnel, documentary protection, protection of automated information systems and/or networks and cryptographic protection. The level of protection for each personal data register must be defined on the basis of an impact assessment that may require: low, medium, high and extremely high protection with different technical and organisational measures accordingly (see Annex 3 of the Ordinance)

Main regulatory tools addressing security and cybersecurity in Bulgaria

3.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

The Bulgarian Cybersecurity Act envisages obligations and procedures for network and information security applicable to:

1. the administrative authorities;

2. the essential service operators, - for each sector, sub-sector and service indicated in Annex 1, notably energy, health, transport, banking sector and provider of financial infrastructure, potable water, providers of digital infrastructure

3. the digital service providers as provided for in Annex 2, notably online marketplace, online search engine and cloud computing services except where these are SMEs

4. the persons performing public functions, not identified as essential service operators, when these persons provide administrative services by electronic means;

5. the organisations providing public services, who are not identified as essential service operators or are not digital service providers within the meaning hereof, when these organisations provide administrative services by electronic means.

Article 4 states that network and information security measures shall include organisational, technology and technical measures applied according to the specifics of the entities to which the act is applicable and proportional to the threats with the aim to minimise the risk of the threats becoming materialised.

The essential service operators, digital service provider and public authorities are obliged to:

1. take appropriate and proportional measures to ensure a network and information security level corresponding to the existing risk;

2. take appropriate measures to prevent and minimise the impact of incidents affecting their network and information security intended to ensure the availability of their essential services/business continuity;

3. take the measures defined by the ordinance on the minim level of network and information security

4. report incidents to the competent authorities (as explained in the questionnaire below)

The minimum scope of the network and information security measures, as well as any other recommended measures are defined by an Ordinance of the Council of Ministers (SG No. 59 from 26 July 2019) which envisages very detailed minimum measures and requirements which are only summarized here per categories:

- Governance of network and information security: Definition of roles and responsibilities; Information security policy; Documentation of the information; Classification of the information; Risk management; Management of information assets; Human resources security; Management of communications with third parties; Updates management; Security in the development and acquisition of new information and communication systems;

- Protection: Segregation; Traffic filtering; Unauthorized use of devices; Encryption; Management of information and communication systems; Administration of environment; Access management; Remote control protection; Hardware protection; Software and firmware protection; Malware protection; Web servers protection; Domain Name System (DNS) protection; Physical security; Protection of industrial systems for control; Monitoring; Logs; Management of incidents with the network and information security; Incident reporting

- Sustainability/continuity: Back-up and archiving of information; Back-up of components of the infrastructure; Business continuity plans

- Control and audits

The Act on the Payment Service and Payment Systems further envisages security obligations for payment service providers (such as credit institutions, account information service providers, payment initiation service providers). Article 98 obliges payment service providers to establish appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide, and establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents. Payment service providers shall provide to Bulgarian National Bank (BNB) an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks. Article 99 further obliges payment service providers authorised by BNB to notify immediately BNB of the occurrence of any major operational or security incident – obligation examined more in detail below in relation to the question for the data breach reporting. BNB is obliged to issue an ordinance for the procedure and requirements to comply with these two provisions, but such ordinance is yet to be adopted.

The Act on Electronic Communications further empowers the CPDP to check compliance with the following obligations that undertakings providing public electronic communication networks and/or services must comply with:

1. the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

2. ensuring appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure;

3. ensuring appropriate technical and organisational measures to ensure that the data can be accessed by specially authorized personnel only;

4. the data, except those that have been made available to the competent authorities and have been preserved thereby, shall be destroyed at the end of the period of retention, except in the cases expressly provided for by the law.

Respectively, the Commission for Personal Data Protection shall have the right to:

1. acting within the competence thereof, require information from the undertakings providing public electronic communications networks and/or services;

2. issue binding instructions, which shall be subject to immediate execution.

Annually, not later than the 31st day of March, the undertakings providing public electronic communications networks and/or services shall provide the Commission for Personal Data Protection, in its capacity as supervisory authority, with statistical information on:

1. the cases in which data have been provided to the competent authorities under Article 251c (1) and (2) and Article 251d (7) herein;

2. the time elapsed between the initial date on which the data were retained and the date on which the competent authorities requested the transmission of the data;

3. the cases where requests for data could not be met.

Specific obligations for reporting of personal data breaches and powers of CPDP to audit the technical and organisational measures are also envisaged as examined in the questionnaire below on the personal data breach reporting.

(ii) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

The NIS Directive is transposed in Bulgaria with the Cybersecurity Act and the Ordinance on the minimal level of network and information security (examined above). However, even if there are laws and regulations in Bulgaria in the field of cybersecurity, recent problems with the continuity of the Commercial register (which completely stopped working for more than a week in August 2018), the recent breach in the National Revenue Agency of the tax data of over 5 million Bulgarians and a number of other security breaches (e.g. in the sector of education, banking and others) show that the implementation and enforcement of these regulations is very poor. In October 2019, the European Commission has also started infringement proceedings against Bulgaria (with formal notice) for failure to transpose properly the NIS Directive, in particular regarding certain offences and the respective penalties - see https://europa.eu/rapid/press-release_INF-19-5950_en.htm?cookies=disabled.

(iii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

Before 25 May 2018 (when GDPR entered into force), there was an Ordinance on the minimal level of technical and organisational measures and the permissible data processing (see table above with text of the ordinance available in English), but this Ordinance is now repealed. On its website, the CPDP has committed to transform the ordinance into soft-law/guidance for data controllers, but this is yet to be done, so currently there are no particular soft or hard-law provisions requiring certain technical or organisational measures in implementation of the GDPR.

3.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

The Cybersecurity Act does not speak about ‘data breach’, but obliges public authorities to inform the respective security incidents response teams within 2 hours after the incident detection about ‘incidents having impact on their business continuity’. The same obligation is applicable also to:

- Persons performing public functions and organisations providing public services for ‘incidents having impact on the availability of the electronic service provided’;

- Providers of essential services for ‘incidents having impact on the availability of their essential services’;

- Digital service providers for ‘incidents having substantial impact on the availability of their digital services’ where the following criteria shall be considered to identify the impact as substantial:

1. the number of users affected by the incident and, more specifically, the number of users relying on the service to provide their own services;

2. the incident duration;

3. the territorial scope with regard to the area affected by the incident;

4. the degree of service disruption;

5. the degree of impact on the business and public activities.

A standard form should be used for this reporting as provided for in the Ordinance on the minimal level of network and information security and the ENISA classification followed in assessing the type and severity of the incident (annexes 7 and 9 of the ordinance). Within 5 business days, the organisation shall provide to the sector team the full incident information defined by the ordinance. Upon justified assumption that the reported incident can be classified as a computer-related crime, the sector team shall notify the General Directorate for Combatting Organised Crime within the Ministry of Interior.

Article 24 of the Cybersecurity Act obliges the respective computer security incident response team to provide, upon request, to the organisation submitting an incident notification, the appropriate information related to the follow-up actions on the notification, including any information which could help the effective incident response. Upon consultation with it, the respective computer security incident response team may inform the public about individual incidents, when public awareness is required to prevent an incident or address an existing incident.

Article 99 of the Payment Service and Payment Systems Act further obliges payment service providers authorised by Bulgarian National Bank (BNB) to notify immediately BNB of the occurrence of any 'major operational or security incident'. Where the incident has or may have an impact on the financial interests of payment service users, the payment service provider shall immediately inform its payment service users of the incident and of all measures it takes to limit the adverse effects of the incident. Upon receipt of the notification for an incident, BNB shall provide in a timely manner the relevant details of the incident to European Banking Authority (EBA) and to the European Central Bank (ECB). The BNB can also notify other competent authorities in the territory of the Republic of Bulgaria and, where necessary, take actions with the purpose of protecting the financial system. Payment service providers authorised by BNB shall provide BNB with statistical data on fraud relating to payments. The BNB shall provide EBA and the ECB with this data in an aggregated form. The BNB shall issue an ordinance on the application of Article 98 and of this Article - yet to be done.

Although the Cybersecurity Act and the Act on Payment Services use the terminology of 'incident', it is clear that where an 'incident' affects at the same time personal data, the breach should be also classified as a 'personal data breach' and should be reported to the CPDP and possibly the data subjects in accordance with Articles 33 and 34 GDPR. In this respect, Article 16(12) of the Cybersecurity act specifically obliges the national competent authorities on cybersecurity to cooperate with the personal data protection authorities working on any incidents resulting in a data security breach. However, the Bulgarian legislation does not contain any additional to the GDPR requirements for notification of 'personal data breaches' to CPDP except for breaches in the electronic communication services.

Article 261c of the Act on Electronic Communications envisages that in case of a 'personal data breach', the undertaking providing public electronic communications services shall notify the Commission for Personal Data Protection within three days after detection of the breach. Where the breach is likely to adversely affect the personal data

or privacy of a subscriber or another person, the undertaking shall also simultaneously notify the subscriber or person concerned of the breach detected. Notification of the breach referred to the subscriber or the other person affected shall not be required where the undertaking has demonstrated to the Commission for Personal Data Protection that the said undertaking has undertaken appropriate technical measures for protection of the personal data concerned by the breach. Such measures shall render the data unintelligible to any person who is not authorised to access it. In case the undertaking has failed to notify the subscriber or the person affected by the breach, the Commission for Personal Data Protection, having considered the likely adverse effects of the said breach, may require the undertaking to notify the person concerned. The notification to the subscriber or the person shall at least describe: 1. the nature of the consumer's personal data breach; 2. the contact points where more information can be obtained; 3. recommended measures to mitigate the possible adverse effects of the subscriber's or natural person's personal data breach. In addition, the undertaking providing public electronic communications services shall furthermore indicate the following in the notification of a personal data breach to the CPDP: 1. description of the consequences of the personal data breach; 2. the measures proposed or taken by the undertaking to address the breach.

Article 261d obliges the CPDP to issue instructions concerning the circumstances in which the undertakings providing public electronic communications services notify consumers of their personal data breaches, the format and the manner of such notification. This has been done with the Ordinance № 1 from 21 December 2016 for the circumstances where the undertakings providing public electronic communication networks and/or services shall notify users about personal data breaches, the form and means of the notification.

CPDP may audit whether the undertakings have complied with the notification obligation and to impose sanctions upon non-compliance. CPDP may also audit the technical and organisational measures taken by the undertakings providing public electronic communications networks and/or services and may issue recommendations about the best practices concerning the level of security which should be achieved. Article 261e obliges the undertakings to maintain an inventory of consumers' personal data breaches, including the facts surrounding the breach, the effect thereof and the remedial action taken.

3.3.4 Supervision of cybersecurity

(i) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

Yes, a couple of national competent authorities have been appointed with a decision of the Council of Ministers to be in charge of the enforcement and oversight of the Cybersecurity Act:

1) State Agency for e-Governance - responsible for all public authorities and persons performing public functions and organisations providing public services through electronic services

2) Ministry of Health - responsible for the Health sector (Healthcare facilities, including hospitals and private clinics)

3) Ministry of Transport, Information Technology and Communications – responsible for the transport sector (road, air, railway water), the providers of digital infrastructure and the digital service providers (online marketplace, online search engine and cloud computing services)

4) Ministry of Energy – responsible for the energy sector (electricity, oil, natural gas)

5) Ministry of Regional Development and Public Works – for the delivery and supply of potable water

The powers of these competent authorities are defined in Art. 16 of the Cybersecurity act:

1. coordinate and control the performance of all network and information security tasks of the administrative authorities, essential service operators and digital service providers hereunder;

2. adopt, upon endorsement by the State e-Government Agency, guidelines on the circumstances whereupon the entities under Article 4 (1) shall notify about incidents;

3. assess whether the administrative authorities, essential service operators and digital service providers perform their obligations under Chapter Two, as well as the impact of their performance on the network and information security, and take the appropriate measures upon any identified cases of non-performance;

4. jointly with the European Union Agency for Network and Information Security (ENISA), create recommendations and guidelines related to the technical areas to be considered with regard to the application of the relevant European or international network and information security standards;

5. with the assistance of the European Union Agency for Network and Information Security (ENISA), create recommendations and guidelines with regard to the application of existing, including national, standards aimed at the uniform application of Chapter Two.

The national competent authorities shall ensure that the computer security incident response teams receive incident notifications hereunder.

The national competent authorities may request from the administrative authorities and essential service operators:

1. any information required to assess their network and information security, including existing security policies, results of network and information security audits performed by another qualified auditor and the underlying evidence;

2. evidence of their effective implementation of the network and information security audit recommendations.

In their requests, the national competent authorities shall indicate the purpose and the specific information or evidence being requested. Upon assessing the information or evidence, the respective national competent authority shall, as appropriate, provide mandatory instructions to clear the identified omissions in the performance of the requirements provided for in Chapter Two. For the purposes under Chapter Two, the national competent authorities may request the digital service providers to:

1. provide the information required to assess their network and information security, including any existing security policies;

2. correct any omission in the performance of the requirements provided for in Chapter Two.

Upon receiving evidence that a certain digital service provider has failed to meet the requirements set under Chapter Two, the respective national competent authority shall take action in accordance with its powers above. Such evidence may be provided by a

competent authority of another Member State of the European Union wherein the digital service provider provides the respective service.

The national competent authorities may request from the computer security incident response teams any information under item 1 of Article 17 (4) and (7). The national competent authorities shall assist the National Point of Single Contact in the performance of its functions under Article 17 (2), (3), (4) and (7).

The national competent authorities shall cooperate with the personal data protection authorities working on any incidents resulting in a data security breach.

The national competent authorities shall have the technical, financial and human resources required to ensure their ability to effectively perform their tasks assigned hereunder.

Under sectoral legislations, responsible supervisory authorities for cybersecurity identified in addition are:

1) the Communications Regulation Commission - responsible for the security of the electronic identification and trust services for electronic transactions under the Act on electronic identification and trust services

2) the Commission for Personal Data Protection – responsible for the security and confidentiality of the public electronic communication networks and/or services under the Act on Electronic Communications

3) the Bulgarian National Bank – responsible for the security of the banking sector and the providers of payment services under the Act on Payment Services and Payment Systems

(ii) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or something similar established? If yes, what are the competences and responsibilities?

In Bulgaria, there is no single body/institution responsible for cybersecurity, but a range of competent public authorities with enforcement powers as detailed in the reply above. In addition to these competent national authorities, it may be relevant to mention also the powers of the Chairperson of the State Agency for e-Governance and the State Agency for National Security.

The powers of the Chairperson of the State agency for e-governance are defined in Article 12 of the Cybersecurity Act as follows:

1. implement the government network and information security policy;

2. create and propose for adoption by the Council of Ministers a National Network and Information Security Strategy;

3. issue methodological guidance and coordinate the implementation of the network and information security policies;

4. certify the compliance of the information systems deployed by the administrative authorities with the network and information security requirements and exercise control over the administrations to ensure compliance with these requirements;

5. exercise control to ensure the administrative authorities' compliance with the network and information security requirements;

6. conduct, through persons authorised thereby, information security audits of a specific information system or of the measures taken by the administrative authority and issue directions for their improvement;

7. develop methodology and rules to assess the compliance with the network and information security measures defined by the ordinance on the minimal level of NIS measures;

8. coordinate, organise and conduct international and national network and information security exercises and drills

The powers of the State Agency for National Security are defined in Article 15 of the Cybersecurity Act. The Agency shall implement the policy of protection against cyberincidents within the communication and information systems of the strategic locations and activities of significance for the national security. The State Agency for National Security shall establish and maintain a Monitoring and Response Centre for incidents having significant damaging impact on the communication and information systems of the strategic locations and activities of significance for the national security. The Centre shall:

1. monitor and gather information on events and incidents related to the security of the communication and information systems of the strategic locations and activities of significance for the national security;

2. submit alerts on cyberthreats and information on cyberincidents to the strategic locations and activities of significance for the national security;

3. provide methodological assistance in the cyberincident management process;

4. provide a comprehensive analysis of the incoming information and an assessment of the information protection of the strategic locations and activities of significance for the national security.

The Centre shall maintain readiness for a coordinated joint response, within the National Cybersecurity Coordination and Organisation Network, upon any incident related to the security of the communication and information systems of the strategic locations and activities of significance for the national security. It shall further perform tasks related to the functions of the State Agency for National Security under Article 6 (5) of the State Agency for National Security Act.

Upon notification by the State Agency for National Security, the managers of strategic locations, the contracting authorities and the contractors of strategic activities shall, as soon as technically possible, filter or block the malicious Internet traffic - source of cyberattack.

(iii) How can damages caused by lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

Article 39 of the DPA states only that 'in the judicial proceedings, the data subject may claim compensation for the damage suffered as a result of an unlawful processing of personal data from the data controller or processor' - emphasis added as this seems rather restrictive in comparison with Article 82 GDPR which envisages a right to compensation for any infringement of GDPR. The Cybersecurity Act also does not envisage any special regime for compensation of damages caused by lack of cybersecurity. Nevertheless, such damages could be claimed under the general requirements of tort law /non-contractual liability under article 45-54 of the Act on Obligations and Contracts – 'Every person must redress the damage he has guiltily caused to another person. In all cases of tort guilt is presumed until proven otherwise'. Compensation shall be due for all material and immaterial damage which is a direct and immediate consequence of the tort. It may be payable as a lump sum or in regular instalments. If the person suffering the damage has contributed to its occurrence, the compensation may be reduced. Compensation for a personal tort (immaterial damages) shall be determined ex aequo et bono by the court. If the damage is caused by several persons, they shall be liable jointly and severally. A person liable for a damage caused guiltily by another is provided with an action against the latter for what was paid.

If there is a specific obligation in the contract to ensure the security and confidentiality of the data, damages may be claimed instead as part of the contractual liability under article 79-83 of the Act on Obligations and Contracts. Damages under contractual liability shall cover the losses suffered and the loss of profit as far as they are a direct and immediate consequence of the non-performance and could have been foreseen upon the arising of the obligation. However, if the debtor under the contractual relation has acted in bad faith, he shall be liable for all direct and immediate damages. If the non-performance is due to circumstances for which the creditor is responsible, the court may reduce the damages or exempt the debtor from liability. The debtor shall not owe damages for losses which the creditor could have avoided with due diligence.

If the damage is caused by a public authority in the exercise of its administrative activity, there is a special regime for liability under the Act on the Liability for Damage Incurred by the State and the Municipalities. Article 1 states that the State and the municipalities shall be liable for any damage inflicted on individuals and legal persons by legally non-conforming acts, actions or omissions of State bodies and municipal authorities and officials upon or in connection with the performance of administrative activity. In these cases, the State and municipalities shall owe compensation for all damage to property or any other damage being the direct and immediate consequence of damaging behaviour and regardless of whether inflicted by the officer concerned in a culpable manner. State and municipalities can be released from liability only: 1. if the damage had resulted on account exclusively of the victim's culpable behaviour, no compensation shall be owed, or 2. where the victim had contributed to the damage in a culpable manner, the compensation owed shall be reduced. Under the Act on the Liability for Damage Incurred by the State and the Municipalities, the injured person bringing the action against the state/municipality shall pay a more privileged regular state courts' fee of 10 BGN (5 euro) for natural persons and 25 BGN (12,5 euro) for legal persons. No litigation costs, nor enforcement ones, shall be payable in advance.

3.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

Computer crimes are regulated in Articles 319a-f of the Criminal Code and they are almost always punished by both a fine and imprisonment (commutatively). Other crimes that may be relevant for data protection could be possibly:

- Defamation and insult (Articles 146-8a) punished by a fine and a public reprimand
- Systematic stalking (144a Article) punished by imprisonment or probation
- Betrayal of secrets (Article 145) punished by imprisonment or fine
- Use of information collected by special intelligence devices for purposes other than protection of the national security or for the purposes of penal proceedings (Article 145a) – punished by imprisonment and a fine
- Violation of the inviolability of correspondence (Article 171) punished by imprisonment and a fine
- Acquisition, storage, disclosure or dissemination of data as those collected, processed, kept or used as per the Electronic Communications Act (Article 171a) punished by imprisonment or probation
- Impeding someone to take a job, or compelling him to leave a job because of his nationality, race, religion, social origin, membership in a trade union or another type of organization, political party, organisation, movement or coalition with political objective, or because of his or of his next-of-kin political convictions (Article 172) - punished by imprisonment or a fine
- Copyright crimes (articles 172a-174) punished by imprisonment and a fine
- Fraud (Article 213) punished by imprisonment or probation for minor cases
- Blackmail (Article 213a) punished by imprisonment and a fine
- Forgery and other document related crimes (Articles 308 – 316) – most often imprisonment
- Impersonation (Articles 317-318) – imprisonment, or corrective labour, or a fine (alternatively)
- Destroying, hiding or damaging document of another, or document not belonging exclusively to him, for the purpose of causing harm to someone else, or to procure benefit for himself or for another (Article 319) – punished by imprisonment or corrective labour

It may be interesting to mention that the recent hacker attack that caused the data breach in the National Revenue Agency of the data of over 5 million Bulgarians was qualified by the Bulgarian Prosecution as terrorism where the computer crime was deemed committed for the special purpose of 'causing disturbance and fear among the population'. Terrorism is punished between 5 to 15 years of imprisonment. If you are interested in the punishment of other specific crimes, please specify.

(ii) Are there administrative fines related to data protection issues?

Administrative fines related to data protection issues are envisaged in:

1. The Data Protection Act – the administrative fines for non-compliance with certain provisions in the DPA equal the range of fines under Article 83 (4) and (5) GDPR. For non-compliance with other provisions the fine or pecuniary sanction is up to BGN 5,000. For repeated violation double of the amount, initially imposed.

2. The Cybersecurity Act – for failure to properly report an incident within the time limit the fines are between BGN 1,000 and 10,000 and for repeated violation between BGN 2,000 and 20,000 for public authorities. The fines for legal persons are between BGN 1,500 and 15,000 and for repeated violation BGN 5,000 and 25,000 for legal persons. The same fines are also applicable for failure to provide information or perform instructions given by the competent national authorities on cybersecurity. Any official either found in or allowing any other violation under Chapter Two shall be fined between BGN 1,000 and 10,000, unless the violation constitutes a crime and for repeated violation between BGN 1,500 and 15,000.

3. The Electronic Communications Act - Article 327 and the subsequent articles provide for a number of circumstances where administrative fines can be imposed for data protection/confidentiality infringements generally between 1000 BGN and 25 000 BGN.

The CPDP has imposed so far two big fines:

- a fine of 5,1 million BGN imposed on the National Revenue Agency for the personal data breach of the tax data of 5 million Bulgarians. The NRA stated that it will appeal the fine as it considers itself not responsible for the breach which was caused by an external hacker attack. Meanwhile, a number of tax authorities of other Member States (e.g. Germany, Belgium, Austria) stopped the exchange of data with the Bulgarian NRA, considering the exchange of personal data of their citizens as not sufficiently secure.

- a fine of 1 million BGN imposed on the DSK Bank for the theft of the credit files of 33492 clients of the bank - a citizen found by accident the data in a hard disk on the street.

(iii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request?

It depends on the 'type' of data protection offence. In Bulgaria, there are three different ways to prosecute offences:

1. Offences prosecuted only privately by the injured party in judicial proceedings (no involvement of the Prosecution unless the plaintiff is incapable). Offences prosecuted privately include:

- Defamation and insult
- Betrayal of secrets
- Some copyright crimes
- Theft, appropriation and blackmail, where the object of the crime has been private property, if the aggrieved party is a spouse, relative to the culprit of ascending or descending line or of collateral line to the second degree, or a person who lives together with him within one common household, or if the aggrieved party has been guardian or custodian of the culprit.

2. Offences prosecuted officially by the Prosecution, but only at the request of the injured party such as:

- Systematic stalking
- Some copyright crimes
- Impeding someone to take a job, or compelling him to leave a job because of his nationality, race, religion, social origin, membership in a trade union or another type of

organization, political party, organisation, movement or coalition with political objective, or because of his or of his next-of-kin political convictions

3. Offences prosecuted officially by the Prosecution (ex officio - no need for request/complaint by the injured party). All offences that are not explicitly prosecuted under point 1 or 2 are officially prosecuted. In principle, these include all serious offences such as computer crimes, document related crimes, fraud etc.

3.5 Governance

(i) At least in the biomedical sciences research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

As already mentioned in part 1 of the questionnaire, ethical codes and review boards normally exist within each university/research organisation, but these codes and board reviews usually don't focus on privacy/data protection issues except in the case of medical research

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

As already mentioned in part 1 of the questionnaire, state-funded research in Bulgaria needs to be ethical in principle, but in practice there are no special requirements or self-assessment tools that research projects have to undergo to comply with this general principle.

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

Not found in the existing public documents/legislation.

4 Croatia

Sunčana Roksandić Vidlička (University of Zagreb)