Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Bulgaria
Djingov, Gouginski, Kyutchukov & Velichkov

chambers.com

2019

Law and Practice

Contributed by Djingov, Gouginski, Kyutchukov & Velichkov

Contents

Djingov, Gouginski, Kyutchukov & Velichkov is one of the largest Bulgarian law firms and provides full-scope legal services. DGKV's data protection team does audits for GDPR compliance, assists clients with preparation and updates of RoPa and the implementation of appropriate legal measures for personal data protection, advises clients on compliance and responds to specific inquiries under the GDPR. Most of the firm's clients are international business organisations or foreign corporate investors in Bulgaria, ranging from large corporations to mid- and small-size companies, coming from various industries such as telecoms, IT, financial, pharma, production, utilities supply, and data services. The DGKV data privacy team comprises ten lawyers, three partners, four senior and three junior associates. The firm very often provides legal services under a mandate from, or in close co-operation with, a top international law firm. All DGKV data protection lawyers have expertise and experience in at least one other area of law – including telecoms, technology, pharma, health regulation, M&A, financing, banking, employment, etc.

Authors

Violetta Kunze is a partner at DGKV and head of the firm's Telecoms, Media and Technology Practice. Her main focus areas are: telecommunications, technology, data protection and cybersecurity; she has additional expertise in media, corporate law, M&A and commercial contracts. Violetta is a member of the Sofia Bar, the International Bar Association in London, the Communications Law Committee, of which she is co-chair, the South-western Legal Foundation, Dallas, the German-Bulgarian Lawyers' Association, Hamburg, and the German-American Lawyers' Association, Berlin. Violetta also acquired valuable experience moderating panel discussions on data protection and data privacy issues at the 2017 IBA Annual Conference in Sydney, Australia and the 2018 IBA Annual Conference in Rome, Italy.

Ralitsa Gougleva is a senior associate, and co-heads DGKV's Data Protection Practice. She has more than ten years of active legal work as a data protection lawyer. Her main focus areas are: data protection, M&A and general corporate; she has additional expertise in financing and commercial contracts. Ralitsa is a member of the Sofia Bar and the International Bar Association. In 2018, she provided industry-specific training in GDPR compliance to members of the Bulgarian Chamber of Architects and Chamber of Notary Publics and participated as a presenter or panelist in several national and international conferences focused on data privacy and the GDPR.

1. Basic National Legal Regime

1.1 Laws

Since 25 May 2018, the primary legal act regulating data privacy in Bulgaria has been the General Data Protection Regulation (GDPR). The GDPR has direct effect in Bulgaria and its rules prevail over any conflicting piece of Bulgarian legislation. The GDPR regulates the processing of personal data of individuals by organisations with the aim of protecting individuals in respect of their privacy and safeguarding their personal data. The right to personal data protection is one of the fundamental rights and freedoms of individuals under EU law.

Pursuant to the GDPR, organisations may process personal data either as data controller or as data processor. While data controllers are organisations that determine the means and purposes of the processing of personal data, data processors are organisations that process personal data for and under the instruction of a data controller. The GDPR protects privacy right of individuals by imposing obligations to data controllers and processors and setting out enforcement mechanisms.

The GDPR also aims to create a balance between the free movement of personal data within the EU, which is not only important for organisations but also for the protection of natural persons with regard to the processing of their personal data.

The Personal Data Protection Act (PDPA) is the Bulgarian primary legislative act in the area of data privacy. It was amended only recently – amendments came into effect on 1 March 2019 – to set out derogations and other additional and/or specific data protection rules to the GDPR. The amended PDPA also sets out the powers and duties of the Bulgarian Commission for Personal Data Protection (CPDP).

At present, basic data protection laws in Bulgaria include the GDPR and the PDPA. The basic legal framework also includes the Electronic Communications Act (ECA), the

Law on Electronic Commerce (LEC), the Consumer Protection Act and the Access to Public Information Act. Relevant enforcement rules and procedure are set out in the Administrative Procedure Code and the Administrative Breaches and Sanctions Act.

1.2 Regulators

Primary legislation in Bulgaria is within the exclusive competence of the National Assembly of the Republic of Bulgaria.

The CPDP is the principal secondary regulator in the area of data protection. It is a collective state body including a chairperson and four members. The CPDP is an independent supervisory and regulatory authority and its members are appointed by and report directly to the National Assembly of the Republic of Bulgaria; the CPDP is headed and represented by its chairperson.

The CPDP has comprehensive regulatory and promotional powers in the area of data protection. It has all the powers of a national supervisory authority under the GDPR and, in addition it is also competent to undertake the following in the area of personal data protection:

- regulation;
- ensuring the implementation of the decisions of the EU Commission and European Data Protection Board (EU Board);
- participating in international co-operation with national supervisory authorities and in international organisation;
- participating in the negotiations and conclusion of bilateral and multilateral agreements and treaties;
- organising, co-ordinating and holding educational and training sessions;
- issuing administrative acts (within its competency under the law); and
- issuing guidelines, instructions, opinions and best practices.

1.3 Administration and Enforcement Process

The CPDP is the national supervisory authority. Its enforcement powers are set up in the GDPR. The PDPA further specifies that the CPDP shall undertake supervision inspections at its own initiative, upon the appeal of a data subject with a legitimate interest or upon a breach or other signal to the CPDP. The CPDP will issue a decision on any case for which it has opened proceedings and which it has reviewed. Decisions of the CPDP may be subject to court appeal at two instances: first instance before the Administrative Court of the City of Sofia and second instance before the Supreme Administrative Court of the Republic of Bulgaria. The CPDP's terms and procedure of supervision inspections are still to be developed and enacted into an instruction (a piece of secondary legislation). In any case, however, general rules of administrative and administrative penal process govern the enforcement procedures and the due process rights of data controllers and processors in the enforcement process.

All data controllers and processors are subject to the supervision of the CPDP, save for the Bulgarian courts and prosecution and investigation state bodies (collectively, the judiciary), when processing person data as part of the Bulgarian judicial system. GDPR and PDPA compliance by the judiciary is subject to the supervision and enforcement of an inspectorate with the Supreme Judiciary Counsel in Bulgaria. The inspectorate has the powers and authority in respect of the judiciary that the CPDP has in respect of all other data controllers and processors. The terms and procedure that govern the supervision and enforcement powers of the inspectorate are set out in the Rules of Operation of the Judiciary Act.

1.4 Multilateral and Subnational Issues

Bulgarian national law is in line with EU data protection law. Bulgaria is a party to all relevant multilateral legal instruments operating in the rest of the EU. The chairperson of the CPDP is a vice-chairperson of the EU Board.

1.5 Major NGOs and Self-Regulatory Organisations

Major privacy or data protection non-governmental organisations and industry self-regulatory organisations are still to be developed in Bulgaria.

1.6 System Characteristics

The Bulgarian data protection system is part of the larger EU data-protection system. Adopting and implementing GDPR standards of data protection has been and continues to be difficult in Bulgaria since regulatory and enforcement standards that applied in the area prior to the GDPR effective date were significantly lower than those under GDPR.

As of 1 March 2019, GDPR enforcement by the CPDP seems to be less aggressive than it is reported to be in various other EU Member States.

1.7 Key Developments

During the last 12 months the major development in Bulgaria was the adoption of the amendment law to the PDPA, which was in fact a GDPR-implementation law. Further to that, the public awareness of GDPR principles and their actual application seemingly increased, the CPDP became more active in its regulatory and promotional work, and data subjects became noticeably more active in pursuing their rights.

The CPDP remained non-aggressive in the exercise of its enforcement powers. At the beginning of 2019, the CPDP imposed the first enforcement measure under GDPR to a data controller.

1.8 Significant Pending Changes, Hot Topics and Issues

Following the adoption of the newly amended PDPA, it is now time for the CPDP to pass and implement the relevant secondary legislation, the most important piece of which relates to the terms and procedures under which CPDP will exercise its enforcement powers. Another important piece of secondary legislation is the CPDP regulation concerning accreditation of data protection certifying bodies under Article 43 of GDPR.

Industry codes of conduct have been and still are a hot topic. Another hot topic, specifically for journalists and the media, is the balance between the right to personal data protection and the freedom of expression and freedom of speech and the manner in which such a balance will be struck in the context of personal data protection. It has yet to be seen how the CPDP and the courts will adjudicate on the matter.

It has also yet to be seen how national courts will adjudicate on data protection cases under GDPR and whether or not, and to what extent, they will comply with the CJEU case law in the area.

The CPDP's training of data protection officers is also expected to start within the next 12 months.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Requirement for Appointment of Privacy or Data Protection Officers

Pursuant to the GDPR, data controllers and processors must designate a data protection officer (DPO) under the following circumstances:

- the data controller/processor is a public authority or body (except for courts acting in their judicial capacity) and processes personal data in such capacity;
- the core activities of the data controller or processor consists of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the data controller or processor consists of processing on a large-scale special categories of personal data relating to criminal convictions and offences of data subjects.

In any other cases of personal data processing, the data controller may, but is not required to, designate a DPO.

Where a data controller or processor designates a DPO, the controller or processor must notify the CPDP of the designated DPO. The CPDP maintains a register of data controllers and processors which have designated a DPO, as these are notified to the CPDP.

The role of a DPO is to advise its data controller or processor on GDPR compliance and data privacy. In this respect, the DPO must be knowledgeable, qualified and independent; the GDPR sets out a detailed list of requirements to this effect.

Pursuant to the PDPA, the CPDP will organise, co-ordinate and hold training sessions in the area of data protection, including for professionals who would like to be or are already appointed as DPOs, and will issue certificates to those of them who complete the training. These certificates will have a three-year term of validity and will be renewable if the certificate-holder successfully passes an exam.

Application of Concepts of 'Privacy by Design' and 'Privacy By Default'

The concepts of privacy by design and privacy by default are new to the Bulgarian legal order. They were introduced by the GDPR. During the past 12 months, many Bulgarian business organisations had to be educated in and trained to implement the concepts. At present there are very limited, if any, guidelines by the CPDP and case law, by courts on any of the concepts.

The PDPA has introduced several specific obligations for data controllers by which to implement the privacy by design concept, including (i) the obligations to do a DPIA prior to the initiation of a personal data processing that may create a high risk for the rights and freedoms of data subjects, and (ii) to notify and collaborate with CPDP on the mitigation of such risks, where they are identified as a result of the DPIA, again prior to the start-up of the processing.

Need to Conduct Privacy Impact Analyses

In February 2019 the CPDP approved and made public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment (DPIA) pursuant to the terms of GDPR. The list includes the following kind of processing operations:

- a large-scale and regular processing of biometric personal data for the purposes of unique identification of individual(s);
- genetic data processing for the purposes of profiling which has legal effects on or similarly significantly affects relevant data subject(s);
- location personal data processing with the purpose of profiling which has legal effects on or similarly significantly affects relevant data subject(s);
- large-scale processing of personal data where the data have not been obtained directly from the data subjects and the provision of information to data subjects as required under Article 14 of GDPR is impossible or requires disproportionately large efforts, or may make

the data processing impossible, or materially impede the achievement of the data processing purpose;
- the personal data processing is carried out by a data controller which is not established in the EU but has a GDPR-designated representative established in Bulgaria;
- regular and systemic personal data processing where the notification by the data controller to relevant data subjects regarding any rectification or erasure of their personal data is impossible or requires disproportionately large efforts;
- processing of a child's personal data in relation to the offer of information society services directly to the child; and
- migration of personal data from existing into new technologies where such migration concerns personal data processing on a large scale.

The CPDP has expressly stated that the list is indicative and not exhaustive. The purpose of the list is to assist data controllers in Bulgaria in fulfilling their obligations relating to DPIA and in particular in determining whether or not their personal data processing activity requires a DPIA.

Under the PDPA, where a data processing involves usage of new technologies and may in view of its nature, scale, context and purposes lead to a high risk for the rights and freedoms of relevant individuals, the data controller must carry out a DPIA prior to undertaking the processing.

Need to Adopt Internal or External Privacy Policies
The requirement for adoption of privacy policies by a data controller and/or processor is related to GDPR principles of accountability and transparency and secures the right of data subjects to be informed of the processing of their personal data in a fair and accurate manner.

Privacy policies are documents by which a data controller and, to the extent applicable, a data processor, can demonstrate fulfilment of their obligations to implement appropriate technical and organisational measures to ensure secure and compliant processing of personal data. To be useful, privacy policies must be adequate and proportionate to the relevant data processing and addressees.

Bulgarian data protection law does not categorise privacy policies as internal or external. Rather, it sets out the cases in which internal privacy policies are required and to some extent the content such policies should have. Thus, pursuant to the PDPA a data controller or processor that undertakes personal data processing on a large scale, or involving systematic video surveillance of public areas, must have an internal privacy policy with minimum contents as set forth in the PDPA. The same applies to a data controller employer which uses a whistle-blowing system or introduces a control system relating to premises' access, work time and workplace discipline in respect of its employees. The PDPA also sets the minimum content that these internal policies should have.

The PDPA requires that any data controller informs data subjects about the processing of their personal data in accordance with GDPR. The document by means of which a data controller may do this is a privacy notice or privacy policy.

Requirement to Allow Data Subject Access to Data, and Right to Correct or Expunge
Data subjects are entitled to the following rights in relation to the protection of their personal data:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (right to be forgotten);
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights in relation to automated decision-making and profiling.

Data subjects may exercise their rights only in writing by a standard form application to the data controller, including clear identification of the data subject, description of the request or inquiry to the data controller, contact details and preferred method of communication for the data subject. The application must be dated and signed by the data subject. If the application is submitted by a proxy, the relevant power of attorney or other authorisation document must be enclosed with the application.

The data controller's responsibilities corresponding to these rights are primarily related to the obligation of data controllers to implement and maintain appropriate technical and organisational measures by which data subjects' rights are ensured and relevant personal data protected.

The PDPA sets out only the limited number of exceptional cases in which a data controller is not required to allow data subjects to exercise their rights to access, correction and/or expunge. These are cases in which the fulfilment of the corresponding obligation by the data controller may put at risk:

- the national security of the country;
- the defence of the country;
- the public order and security;
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public order and security;
- other important objectives of general public interest, including monetary, budgetary and taxation matters, public health and social security;

- the protection of judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- the protection of the data subject or the rights and freedoms of others; and
- the enforcement of civil law claims.

In all these cases the data subject's rights to data access, correction and/or erasure may be restricted if the terms and procedure of the restriction are set out in the law. One of the areas in which the restriction is fully set up in terms of specific conditions, requirements and procedure is the processing of personal data for journalistic purposes or for the purposes of academic, artistic or literary expression. Relevant terms, conditions and procedure are set out in the PDPA.

Use of Data Pursuant to Anonymisation, De-identification, Pseudonymisation

Anonymous data (ie, data that does not relate to an identified or identifiable individual) is not personal data and is not subject to the GDPR, PDPA or any other data protection regulation. The CPDP has not yet issued any rules or official guidelines on anonymisation of data. However, Opinion 05/2014 on Anonymisation Techniques of Article 29 Data Protection Working Party, adopted on 10 April 2014, may still be used as a helpful tool on the matter. According to the Opinion, data is anonymous when the data is such as not to allow the data subject to be identified via all likely and reasonable means.

Pseudonymised data, on the other hand, is still personal data and is therefore subject to data protection rules. Data is pseudonymised when the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately. Pseudonymisation is a measure that data controllers may use to limit privacy risks. It is a recognised safeguard of data protection and its implementation indicates GDPR compliance.

Concept of Injury/Harm

A data subject whose personal data have been processed unlawfully is entitled to claim damages from the data controller or processor whose non-compliant processing has caused the damages incurred or suffered by the data subject. Relevant damages may be material or non-material but they must result directly from the defendant's infringement of the GDPR or PDPA. In a potential litigation the establishment of the alleged infringement would be a condition for the review of the damages claim and the court would have to resolve on the infringement prior to adjudicating on the damages claim. Once the infringement is established, however, the data controller will be directly liable for the damages caused by the relevant processing and the data subject will not need to prove the incurrence of the damages. The amount of the awarded compensation would be determined by the court based on an expert valuation in respect of monetary damages and at its own just discretion in respect of non-monetary damages. Bulgarian courts created consistent case law on the matter even prior to GDPR coming into effect.

A data subject is entitled to this remedy separately and in addition to the enforcement sanctions that the CPDP may impose on a data controller or processor for the infringement that gives grounds for the damages claim. The PDPA, however, disallows a data subject from claiming damages in court on the grounds of an infringement for the establishment of which an administrative proceeding is pending before the CPDP or the competent administrative court of appeal until such proceedings are pending.

2.2 Sectoral Issues

Sensitive Data

Personal data which are, by their nature, particularly sensitive merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms of individuals. Such 'sensitive' data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of an individual as well as genetic data, biometric data used for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

Under GDPR all these are special categories of personal data and their processing is generally prohibited. It is allowed on an exceptional basis subject to stricter terms and conditions than those applicable to the processing of standard personal data. For example, the processing of a special category of personal data – such as data concerning health or biometric data – would be lawful where the data subject gives his or her explicit consent or the processing is necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or for the protection of vital interests of the data subject.

Processing of special categories of personal data is also subject to greater security measures.

Health Data

Under the Bulgarian Health Act (HA), health data includes not only data concerning health as defined in the GDPR, but also any information contained in medical prescriptions, protocols, certificates and other medical documents. So defined, health data is treated as a special category of personal data.

Apart from healthcare service-providers, employers and insurers licensed to maintain a life insurance portfolio are also allowed to collect and process heath data for specific

purposes related to their rights and obligations under the law.

As of the beginning of 2019 the HA envisages the creation of a National Health Information System with the Ministry of Health, aiming to ensure that the data provided in relation to each citizen's health is full and correct. Access to this system is not only provided to citizens with respect to their own health profiles but also to hospitals, insurers and state bodies that have been authorised to review the data by the Bulgarian law.

Processing of health data is regulated by various pieces of secondary legislation issued under the HA. These are not yet updated to implement the higher standards of protection and enforcement under GDPR.

Communications Data
Pursuant to Article 134 of the ECA, organisations that provide electronic communications services to the public must ensure the possibility of data portability with respect to the numbers of their subscribers, ensuring they could retain those numbers should they decide to switch to a different provider.

Other Categories of Sensitive Data
In general employers only gather information about the union membership and religion of their employees. Both kinds of data are necessary in order to ensure the data subject's employment rights. As for sexual orientation, political or philosophical beliefs, the practice is for such information not to be disclosed to employers.

Profiling is mostly used in marketing, evaluation of ability to receive a bank credit, recruitment, etc. However, as profiling by definition involves a high degree of risk for the rights and freedoms of individuals, it shall not lead to discrimination of persons on the basis of their racial or ethnic origin, political views, religious or philosophical beliefs, union membership, sexual orientation, etc. Another important restriction to note is that no profiling whatsoever is permitted with respect to minors.

Voice telephony
Under Article 261(2) of ECA, any entity that has received data in relation to the provision of services and/or products to consumers may use that data to contact the consumers, including via text messages, for the purposes of marketing and advertising of its own similar services and/or products, provided that it gives each consumer the option to opt out easily from receiving any future messages for any such purpose.

For those entities that offer public telephony services, there is a requirement under Article 257(9) of the ECA to obtain the prior explicit consent of their subscribers before providing access to their network for the purposes of making calls, sending text messages and e-mails to companies that engage in direct marketing and advertising.

Further, pursuant to Article 308 of the ECA, those entities that offer public electronic messaging networks and/or services, must ensure there is a way to transmit recorded electronic services to State Agency National Security via fixed lines.

Internet
Privacy policies: pursuant to Article 4a, paragraph (1), item 1 of LEC, any service-provider that stores or is given access to data must provide clear and explicit information to data subjects regarding the protection of their personal data.

Use of cookies, beacons, tracking technology: the LEC allows the use of cookies provided that the online services user has been informed of the use of cookies and he or she has been given the opportunity to refuse the storage of or access to such cookies. The restrictions are not applicable: (i) to any subsequent use of cookies in so far that the user has not explicitly objected to such use; and (ii) if the cookies are used for the sole purpose of carrying out the transmission of a communication over an electronic communication network or for the provision of an information society service requested by the user. At EU level, when the draft ePrivacy Regulation comes into effect it will most probably enhance the current cookie consent requirement by setting it up at least in line with the consent required under GDPR.

'Do not track' considerations: any collection and processing of such personal data requires consent by the data subject provided for a clearly stated specific purpose; consumers need to be able to withdraw their consent in a manner which is as easy as that in which they initially gave it.

Consent required for behavioural advertising: see comments on profiling above. Additionally, note that Recital 71 to GDPR makes it clear that profiling could be permissible when expressly authorised by EU or Bulgarian law for purposes such as fraud and tax-evasion monitoring but should in any case be subject to suitable safeguards. Bulgaria has not adopted any local laws to this effect.

Other issues: pursuant to Article 6 of LEC, unsolicited messages that are sent by a service-provider to the e-mail of a data subject must be clearly labelled as such from the outset.

Video and television
Under the Bulgarian Private Security Business Act, organisations engaged in private security may store video footage from their cameras for two months after the date of the recording. After the expiry of that period, the videos must be deleted.

Further, personal data processing for journalistic, academic or artistic purposes is lawful, so long as a balance is struck between, on the one hand, freedom of expression and right to information and, on the other hand, the right to privacy. Article 25з(2) of PDPA provides guiding criteria to assess whether a balanced approach is present, including the nature of the personal data, the impact that its dissemination might have on the personal life of the data subject, etc.

Social media, search engines, large online platforms
See comments on other sectoral issues above. Persons who engage in hate-speech or in the spreading of abusive material intended to discriminate on racial, national or ethnic grounds can be held criminally liable pursuant to Article 162(2) of the Bulgarian Penal Code.

Children's privacy
Pursuant to PDPA, consent-based processing of personal data of children below 14 years of age may only be done if a valid consent is obtained by the parents or legal guardians of the child.

The PDPA does not regulate the processing of personal data relating to young people aged between 14 and 18 years. In respect of these data subjects, the following general rule of law applies: they have limited legal capacity and the validity of their legal actions and transactions are subject to the prior approval/consent of their parents or legal guardians, except for minor transactions relating to the young person's ongoing and customary needs and except for transactions with financial payment for work. In light of this rule, consent-based processing of personal data of young people aged 14-18 would require, more often than not, the prior consent of their parents or legal guardians.

The CPDP has consistently ruled that education and school data, such as data relating to students' test and exam results, are personal and are therefore subject to personal data protection.

Under Ordinance No 8 of 11 August 2016 regarding Information and Documents of Pre-School and School Education System, directors of educational institutions must retain data subjects' educational records for at least 50 years.

2.3 Online Marketing

At present, there is no legal definition of 'direct marketing' in Bulgarian law. Nonetheless, by interpretation of relevant historical provisions and case law it may be concluded that direct marketing means any communication offering goods or services to individuals or business organisations in any direct manner (by e-mails, SMS, app-based messaging and/or other messaging or by whatever other means) and any survey aimed at researching and/or receiving feedback on offered goods or services.

Where direct marketing involves the processing of personal data it must comply with GDPR in its treatment of that personal data.

In addition, the ECA requires the consent of the individual subscriber (whether an individual or a legal entity) as a condition for lawfully engaging in direct marketing and advertising by e-mail, with or without human intervention; such consent is subject to withdrawal at any time. Additionally, pursuant to LEC, the Bulgarian Commission on Consumer Protection keeps a register of the e-mail addresses and telephone numbers of legal entities which have expressly opposed receiving unsolicited commercial communication. Sending unsolicited commercial communication to those e-mail addresses or making a call to these telephone numbers, including for direct marketing purposes, is prohibited. As an exemption to the rule of ECA, no prior consent is required for cases where the similar products and services exemption rule of EU law applies.

The ECA further prohibits direct marketing and advertising e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) the provided opt-out address is not valid.

Pursuant to LEC, in the case of non-solicited communication, the sender must also include standard e-commerce information.

The use of cookies is regulated by the LEC. The LEC allows the use of cookies provided that the online services user has been informed of the use of cookies and he or she has been given the opportunity to refuse the storage of or access to such cookies. Such restrictions are not applicable: (i) to any subsequent use of cookies in so far that the user has not explicitly objected to such use; and (ii) if the cookies are used for the sole purpose of carrying out the transmission of a communication over an electronic communication network or for the provision of an information society service requested by the user.

2.4 Workplace Privacy

Under GDPR, in respect of processing of employees' personal data in the context of employment, the Bulgarian local regulations may provide for specific rules which shall, however, include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights. If no such local rules are set out in Bulgarian law, GDPR rules continue to apply.

Employers often process the personal data of their employees on the legal basis of their legitimate interests as business organisations. In these cases employers must strike the right balance between safeguarding the employee's human dignity and privacy and ensuring their business legitimate interests

– eg, protection of the work premises, security of communication channels, security of the employer's vehicles, etc.

Special Rules
To introduce and use any of the following workplace arrangements:

- a whistle-blowing system or other system for reporting workplace infringements;
- limitations or restrictions on the usage of the organisation's resources for private or other work unrelated purposes; and/or
- introduction of a monitoring or access control system relating to workplace attendance and discipline.

An employer, as data controller, must approve and adopt internal company rules and procedures regulating the relevant arrangement and the personal data processing that its implementation involves. As a minimum, the rules and procedure must include information about the scope of application and methods of operation of the relevant arrangement and the employees' and employer's obligations in relation thereto. The arrangement should not in any case restrict or impede the data protection rights of employees under GDPR and PDPA. Employees must be notified in a fair and accurate manner by the employer of the adopted rules and procedures prior to their implementation.

The PDPA also sets out that any employer shall determine a term for safekeeping and otherwise processing personal data of job applicants for recruitment purposes. Under the PDPA such a term may not be longer than six months, unless the job applicant has consented in accordance with GDPR to the processing of his or her personal data for a longer period, in which case the personal data of the job applicant may be processed until the expiry of such longer period. Based on this rule, it may further be concluded that an employer may use its legitimate interest as legal basis for the processing of job applicant's personal data provided that the employer limits the data processing for a term of up to six months and that for a lawful processing of the same data for a longer period the employer will have to rely on the data subject's consent or another legal basis.

Monitoring Systems at the Workplace
When employers use video cameras to monitor employees, they must have a legitimate business reason. The employer has a recognised legitimate interest to install video surveillance for security purposes in its premises. However, in the event of telework, the Bulgarian Labour Code explicitly provides that video surveillance can be installed only upon the explicit consent of the employee, expressed in writing.

The employer has to adopt privacy rules, which shall contain procedures related to informing the employees on the fact of monitoring and the types of monitoring invoked in practice – eg, inspection of employees e-mails, video surveillance, etc. In addition, it is essential to place signs indicating the fact of video recording as well as its purpose. Under the Law on Private Security Business Activity, the maximal retention period of video recordings for security purposes is two months as of the date of video recording. Furthermore, video surveillance even for security purposes must be of such character that it should not contradict the principles of confidentiality and transparency established in the GDPR, as well as not being excessive and being focused only on the employee's workplace.

Since the Bulgarian Constitution prohibits any kind of interference in personal correspondence, in the event that the employer would like to monitor the e-mail correspondence of its employees, it is important to incorporate an explicit prohibition on the use of the company's e-mails for personal correspondence. Such prohibition may be incorporated in the internal company rules or set out in a separate document, delivered to the employees and countersigned by the employee for receipt.

As a rule of thumb, in order for an employer's workplace monitoring system to be lawful, the employee must be aware of, and not unduly surprised by, the introduction and manner of operation of the system and of its effects on his or her data privacy.

Role of Trade Unions
Trade-union bodies are statutorily entitled to participate in the drafting of all internal rules and regulations which pertain to labour relations and the employer is obliged to invite them to do so. The employer, however, does not need to accept or incorporate any proposals of trade-union bodies in the privacy rules, nor are the privacy rules subject to their approval or other sanction.

Whistle-blowing Hotlines and Anonymous Reporting
Bulgarian law does not contain any specific rules or regulations on the function of whistle-blowing hotlines and anonymous reporting. Data processing in the context of reporting cases would generally fall into the scope of 'realisation of the legitimate interest of the data controller'. However, it cannot be ascertained that this would apply to any and all allegations reported (eg, if sensitive personal data is processed, the ground of consent will be a more appropriate option for the collection and use of personal data in relation to such reporting practices). Again, it will be necessary to strike a balance between the principles established in the GDPR and the legitimate interest of the employer to ensure labour discipline or/and prevent violations of the law by employees. If such a balance may not be achieved in view of the specific whistle-blowing or other reporting system, the latter will be subject to the employees' prior consent. In any case, these reporting systems have to be incorporated in privacy rules

and the procedure related to functioning of such systems communicated duly to the data subjects.

Anonymous reporting is not explicitly prohibited by law but it is generally not recommended as it may qualify as violating human dignity or other constitutional rights of employees.

2.5 Enforcement and Litigation

The CPDP may supervise data controllers and data processors by inspections commenced at its own initiative, upon a data subject's complaint or upon a third-party's report. The general rules of Bulgarian administrative procedure – or, as applicable in case of established infringements, the administrative penal procedure – governs inspections. At present, dawn raids under GDPR are not regulated in further procedural detail under Bulgarian law. From data controllers' and processors' perspective this implies that in a dawn raid CPDP officials have only the investigative powers that are set out in Article 58, paragraph (1) of GDPR (ie, to access but not to seize relevant premises, documents, equipment, data, etc). A dawn raid is also not subject to prior approval by a prosecutor or judge. Instead, the evidence collected under a dawn raid and the infringement findings established in result of it are subject to a follow-up court review for due process and substantive law lawfulness.

Lawyers' professional secrecy is enforceable against the CPDP investigators.

The obstruction of an inspection by a data controller or processor may trigger an administrative fine for the organisation ranging up to EUR20 million or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher. The responsible organisation's officials may be held personally liable under criminal law and are punishable either by imprisonment for up to three years or by a fine up to EUR1,000. The organisation, as a legal entity, may not be subject to criminal liability.

Enforcement and Penalties

In terms of corrective powers, the CPDP may issue and apply mandatory administrative measures and/or impose administrative sanctions. All measures and sanctions are set out in GDPR. Mandatory administrative measures include warnings, reprimands and orders to a data controller or processor, temporary or definitive limitation on data processing, order for rectification or erasure of personal data or for restriction of processing or for notification to data subjects or for suspension of data flows to a recipient in a third country.

Administrative sanctions in the form of penalties are of two maximum levels. The higher maximum amount is EUR20 million or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher; the standard maximum amount is EUR10 million or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher. The penalty level depends on the established GDPR infringement and on the context of the breach. Under GDPR, the CPDP must take into account a number of factors when determining the applicable penalty level.

In respect of an infringement, the CPDP may decide to issue a mandatory administrative measure only, to impose an administrative penalty only or to apply both types of sanctions together.

The CPDP exercise its corrective powers by issuing decisions. The CPDP's decisions may be subject to judicial review at two instances and, accordingly, may be appealed before the Administrative Court of the City of Sofia, as a first instance, and before the Supreme Administrative Court of Republic of Bulgaria, as a second and final instance.

Enforcement Cases

In February 2019, the CPDP issued its first enforcement decision under GDPR. The sanctioned infringement was plain and standard and committed by a bank as data controller. The bank's official made more than one phone call to an individual who was previously a client of the bank, using the personal data of the individual that the bank had processed in relation to that individual's terminated credit; the purpose of the calls was to make contact with the individual's neighbour, who was a current client of the bank with overdue payments. The CPDP ordered the data controller to terminate the personal data processing in respect of the previous client and imposed upon the data controller a penalty of approximately EUR500 for breach of the principle of purpose limitation under Article 5, paragraph (1), item b of GDPR. The decision was not appealed before court.

Class actions

Class actions in relation to personal data protection are not practised in Bulgaria.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

The PDPA includes a set of rules concerning individuals' privacy protection in relation to the processing of their personal data by competent state authorities for the purposes of prevention, investigation, discovery, prosecution and punishment of crimes. In these cases, the PDPA aims to provide data subjects with the same level of data protection and safeguards as under GDPR unless an express exception is set out in a primary legal act, in which exceptional case the processing is permissible if and to the extent it and its purpose are set out in the law.

3.2 Laws and Standards for Access to Data for National Security Purposes

Powers of enforcement and national security authorities' rights to access personal data are expressly set out in laws. Under the Ministry of Interior Act (MIA), the Ministry of Interior is authorised to process personal data whenever national security, crime prevention, public order or penal proceedings are concerned; indeed, the bodies of the Ministry of Interior may process personal data without the consent of the data subject and may further decide not to inform the data subject about the data processing for its entire duration.

Further, pursuant to the LEC, law enforcement agencies such as the National Police, Chief Directorate Border Police, Directorate Internal Security, etc, may access data gathered by entities that provide electronic communications networks and/or services. However, in order for these agencies to be granted access, the enforcement agency must prepare a motivated request and submit it to the regional court at the seat of the agency that seeks access. If the court sanctions the request, it must explicitly provide which data is to be accessed, the period of time for which data shall be made available and other specific information, designed to reduce unnecessary intrusion into data subjects' privacy and personal data.

3.3 Invoking a Foreign Government

Following the GDPR effective date, an organisation may not invoke a foreign government access request as a legitimate basis to collect and transfer personal data. In relation to such transfer, see section **4. International Considerations**, below.

3.4 Key Privacy Issues, Conflicts and Public Debates

Enforcement acts and decisions are subject to administrative and court appeal to protect individuals' privacy and other human rights from undue processing.

4. International Considerations

4.1 Restrictions on International Data Issues

Transfer (such as disclosure, giving access to, communication, etc) of personal data to a data controller or processor within the EEA is subject to all GDPR rules other than those under Chapter V of GDPR relating to transfers of personal data to third countries or international organisations (third-country transfer). A third country transfer is deemed riskier for the rights and freedoms of data subjects since it is assumed that third countries (ie, countries outside the EEA) and international organisations do not provided the level of data protection that GDPR provides. Accordingly, any such third-country transfer is generally banned. It is permissible only if the terms and conditions set out Chapter V of GDPR are fulfilled. The cases in which a third-country transfer is permissible are as follows:

- the European Commission has decided that the relevant third country or international organisation ensures an adequate level of personal data protection. As of 1 March 2019 the European Commission has recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate data protection, and adequacy talks are ongoing with South Korea;
- In the absence of an adequacy decision by the European Commission, the data controller or processor has provided appropriate safeguards, and on condition that enforceable data-subject rights and effective legal remedies for data subjects are available. Appropriate safeguards can be:
  - (a) a legally binding and enforceable instrument between public authorities or bodies;
  - (b) binding corporate rules approved by the CPDP or, as may be applicable, other competent supervisory authority;
  - (c) standard data protection clauses adopted by the European Commission;
  - (d) if available, standard data protection clauses adopted by a supervisory authority and approved by the European Commission;
  - (e) if available, an approved code of conduct on condition that enforceable data-subject rights and effective legal remedies for data subjects are available;
- in the absence of an adequacy decision by the European Commission and of appropriate safeguards, as summarised above, one of the following conditions applies:
  - (a) the data subject has explicitly consented to the proposed transfer after having been informed of the possible risks of the transfer;
  - (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
  - (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
  - (d) the transfer is necessary for important reasons of public interest;
  - (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
  - (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
  - (g) the transfer is made from a register which, according to EU or Bulgarian law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU

or Bulgarian law for consultation are fulfilled in the particular case;

- where a third-country transfer may not be based on any of the above grounds, it may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the data controller – which are not overridden by the interests or rights and freedoms of the relevant data subject – and the data controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. In this particular case the data controller must inform the CPDP and the data subjects of the third-country transfer;
- a data controller or processor must further document the availability and applicability of the legal basis on which it undertakes and completes the third-country transfer.

4.2 Mechanisms That Apply to International Data Transfers

See **4.1 Restrictions on International Data Issues**, above.

4.3 Government Notifications and Approvals

See **4.1 Restrictions on International Data Issues**, above.

4.4 Data Localisation Requirements

Localisation of data out of the EEA is deemed a third-country transfer and is subject to the restrictions on international data issues discussed above. Appropriate technical and organisation measures that a data controller or processor needs to implement to secure personal data under GDPR must be also appropriate in view of the data location.

4.5 Sharing Technical Details

At present, Bulgarian law does not oblige or allow organisations to install and/or use any software code or algorithm or similar technical detail that is shared with the government.

4.6 Limitations and Considerations

When an organisation is faced with a mandate or request to collect or transfer personal data to another jurisdiction in relation to a foreign government data request, foreign litigation proceedings (eg, civil discovery) or internal investigations then GDPR rules apply. Data transfers within the EEA are free, while to a third country they are subject to additional requirements and safeguards, detailed in **4.1 Restrictions on International Data Issues**, above.

A third-country transfer in response to a foreign government request may prove impermissible if no mutual legal assistance treaty or other relevant international treaty applies. In the case of foreign litigation proceedings, a possible legal basis for the data transfer may be the data controller's legitimate interests, in which case the transfer would be permissible as it is necessary for the establishment, exercise or defense of legal claims. In the case of an internal investigation, a possible legal basis for the data transfer may be the data controller's or third party's compelling legitimate interests, in which case the transfer would be permissible if subjected to appropriate safeguards such as binding corporate rules or standard contractual clauses. Consideration must also be given as to whether the transfer relationship involves two independent controllers or a controller-processor relationship.

4.7 "Blocking" Statutes

As explained above in **4.1 Restrictions on International Data Issues**, a third-country transfer is banned unless it meets certain terms and conditions set out in GDPR. Therefore, the GDPR is the main blocking statute to international data transfers.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

New technologies such as big data analytics, automated decision-making, profiling, artificial intelligence, the internet of things, facial recognition, biometric data, etc, are not specifically regulated under Bulgarian law. Any relevant digital issues in these areas need to be addressed based on GDPR, which applies to all of them. In general, the GDPR assumes that these new technologies are likely to result in a higher risk for the rights and freedoms of individuals and, therefore, requires from data controllers and processors a higher level of protection and security.

For example, emerging technologies more often than not need to pass successfully a DPIA (see 'Need to Conduct Privacy Impact Analyses' in **2.1 Omnibus Laws and General Requirements**) to be implemented and used.

Systems using facial recognition or processing other biometric data are subject to GDPR rules relating to special categories of personal data.

The data subject's consent would often be the applicable legal basis for personal data processing. The data controller's or a third party's legitimate interest may also prove to be a valid legal basis for personal data processing, but these cases would be limited.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

Key Laws

The underlying primary legislative act setting forth the legal framework of cybersecurity in Bulgaria is the Cybersecurity Act (CA), which was adopted very recently, com-

ing into force as of 17 November 2018. It implements the requirements of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive); it envisages measures for implementation of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018, laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council with regard to further specification of the elements to be taken into account by digital service-providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact. ECA, LEC, the Electronic Governance Act, the Act on Management and Functioning of the National Security System, and the Criminal Code also contain relevant provisions. In addition, the Bulgarian Government adopted a National Strategy for Cybersecurity called Cyber Resilient Bulgaria 2020.

The main objective of the CA is to achieve a high level of security where critical infrastructure is involved and to preserve undisrupted operation of the public sector, ensuring consumer trust. The entities which shall apply the network and information security measures under the CA ('obliged entities') are explicitly listed therein, and include:

- the administrative authorities;
- the essential service-operators and the digital services-providers;
- the persons performing public functions, who are not identified as essential service-operators, when such persons provide administrative services by electronic means; and
- the organisations providing public services, which are not identified as essential service-operators or are not digital service-providers, when these organisations provide administrative services by electronic means.

Operators of essential services may be both public and private entities which meet all of the following criteria: (i) the operators provide essential service; (ii) the provision of the essential service depends on networks and information systems; and (iii) any network and information security incident shall have a significant disruptive effect on the provision of the respective service. CA shall apply to operators of essential services which are operating in the sectors listed in Exhibit No 1 to CA (such as energy, transport, banking, financial market infrastructures, healthcare, supply and distribution of drinking water, digital infrastructure), whereas the specific essential service-operators shall be determined in compliance with a methodology to be adopted by the Government. Digital service-providers in turn are those providing any of: (i) an online marketplace, (ii) an online search engine, or (iii) cloud-computing services. With certain exceptions, the CA is not applicable to the undertakings providing public electronic communications networks and/or services under the ECA. Digital service-providers, which qualify as micro-enterprises or small enterprises under the meaning of the Small and Medium Size Enterprises Act, are among the entities which are excluded from the scope of regulation of CA.

Regulators

CA provides for a national cybersecurity system to be established to form part of the national security system and to be managed and organised by the Bulgarian Government. The law sets forth the formation of a Cybersecurity Council – an advisory and co-ordination body to support the Government on cybersecurity matters. The constitution and competences of the Cybersecurity Council are detailed in the CA.

A number of governmental authorities are vested with specific responsibilities and shall exercise their duties to actively counteract cyber-crimes and cyber-crises, such as the Minister of Interior, the Minister of Defence, the State e-Government Agency, the State Agency for National Security, the National Cybersecurity Co-ordinator.

The State e-Government Agency is the national competent authority for all administrative authorities and for the public service organisations that are obliged to apply the measures under the CA. A newly established co-ordinating body – the National Single Point of Contact at the State e-Government Agency – shall be responsible, among others, for the co-ordination of network and information security issues as well as all issues related to the cross-border co-operation at EU level, including with the respective authorities in other EU Member States and the European Commission. A national Computer Security Incident Response Team (CSIRT) with the State e-Government Agency shall assist in reducing the risks of information security incidents and resolving such incidents if they have already occurred. Sector CAIRTs are to be established within competent local authorities in the various sectors (ie, energy, transport, banking, financial market infrastructures, health, and digital) in accordance with the methodological guidelines of the European Union Agency for Network and Information Security (ENISA). Sector CAIRTs shall co-ordinate their activities with the national CSIRT.

The national supervisory authority under GDPR, the CPDP, is not vested with specific powers with respect to cybersecurity issues.

6.2 Key Frameworks

See **6.1 Key Laws and Regulators**.

6.3 Legal Requirements

The 'obliged entities' are required to implement proper cybersecurity measures to ensure for (i) technical and organisational security risk-management of their networks

and information systems, and (ii) measures for prevention and minimisation of security breaches. Under the CA the network and information security measures shall include organisational, technological and technical measures specific to the obliged entities and proportional to the threats. The measures may not require using a specific type of technology.

The minimum scope of the network and information security measures and any other recommended measures shall be defined by an ordinance of the Bulgarian Government that must be adopted within six months as of the entering into force of the CA. As of the current date, that ordinance has not yet been adopted.

ISO 27001 is a commonly recognised standard providing guidance for cybersecurity compliance which is used in Bulgaria, although it is not statutorily required.

Incidents Reporting and Notification under the CA
The obliged entities shall notify the respective sector CSIRT upon any computer security incidents having impact on their business continuity. Initial notification shall be provided within two hours after the incident detection. The notification shall be submitted using a sample form to be set forth in the ordinance of the Bulgarian Government (not adopted yet). The notification shall contain information allowing the sector CSIRT to identify any cross-border impact of the incident. Thereafter, within five business days, the entity shall provide to the sector team the full incident information as the contents of such information shall be defined by a governmental ordinance to be adopted.

6.4 Key Multinational Relationships

The national competent authorities are required to co-ordinate with ENISA technical recommendations and guidelines related to the use of EU or international standards and specifications relevant to network and information security. The National Single Point of Contact at the State e-Government Agency is expected to co-ordinate cross-border co-operation at EU level, including with the respective authorities in other EU Member States and the European Commission. The CA also designates CSIRT as the national counterpart in projects related to the development and testing of EU and NATO standard operating procedures.

6.5 Key Affirmative Security Requirements

The GDPR and PDPA stipulate that personal data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This security principle requires that data controllers and processors take practical steps to ensure protection of personal data. As there is no 'one-size-fits-all' approach, data controllers and processors should carry out a risk analysis in order to determine what measures will be appropriate, taking into consideration the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Based on this analysis, data controllers and processors must choose appropriate organisational and technical security measures to mitigate the risk, taking into account the state-of-the-art and costs of implementation.

The key requirement is ensuring the confidentiality, integrity and availability of personal data. Security measures should seek to guarantee all of these three elements. Pseudonymisation and encryption may be appropriate technical measures.

Data controllers should aim to build a culture of security awareness. They are required to undertake regular testing, assessment and evaluation of the effectiveness of their security measures. The results should be documented, and any recommendations acted upon/safeguards implemented. Furthermore, the organisations must ensure the resilience of their processing systems and services by setting up business-continuity and disaster-recovery plans.

6.6 Data Breach Reporting and Notification

A 'personal data breach' is a wide concept, defined as any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Article 4 (12) of GDPR). The CPDP is the designated Bulgarian authority to maintain the Register for Personal Data Breaches Notifications under Article 33 of GDPR.

In the case of a personal data breach the controller must notify the CPDP (or the Inspectorate) as soon as possible after having become aware of the breach, but not later than 72 hours of the breach. The GDPR contains detailed guidance of what the notification shall contain. When the breach occurs at the level of the processor, the processor shall notify the controller as soon as possible within 72 hours of the breach. Controllers are also required to keep a record of all data breaches including description of the facts related to the breach, the consequences thereof and the remedial measures undertaken.

In more serious cases, when the personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects, the controller shall communicate it to the data subject as soon as possible after becoming aware of the breach. The CPDP may also require such communication to data subjects based on the notification that the CPDP has already received from the data controller in the particular case. The notification to the data subject must describe in clear and plain language the nature of the personal data breach and have a minimum statutory content (Article 34, paragraph 2 of GDPR). There are certain exceptions when

the controller might be exempted from the obligation to notify the data breach to the data subject

6.7 Ability to Monitor Networks for Cybersecurity

All organisations that process personal data or fall within the scope of application of the CA have an obligation to implement appropriate security measures proportional to the relevant threats. In the case of high-risk processing that also means conducting vulnerability tests and investigating potential security breaches. However, since the ordinance setting minimum requirements for network and information security measures has not yet been adopted, currently there is no official guidance on practices or tools for network monitoring and other cybersecurity defensive measures.

6.8 Cyberthreat Information Sharing Arrangements

There is no express statutory requirement to share cybersecurity information with the public authorities. However, all relevant organisations (data controllers and processors, obliged entities under CA) are required by law to report data breaches and cybersecurity incidents respectively. As part of such reporting, certain cybersecurity details would normally be shared.

Voluntary Information-Sharing Opportunities.

Persons and entities that do not fall within the scope of the entities obliged to apply the network and information security measures under the CA may notify the respective sector CSIRTs about incidents having impact on the availability of their services. The notifications of such persons and entities shall be processed by the sector teams only when their processing does not create a disproportionate or unjustified burden. The notifications by the obliged entities shall be processed by the sector CSIRTs with priority.

6.9 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

Recent publicly known cases of significant cybersecurity violations in Bulgaria include the following case. During the municipal elections in Bulgaria in 2015 there was a cybersecurity attack as a result of which the websites of major public institutions such as the Presidency, the Council of Ministers and the Central Elections Commission were blocked. The press reported that it was highly probable the attack was made by the Sofacy Group (aka, 'Fancy Bears'), which was reportedly related to the Russian military intelligence agency. In the recent years, Bulgaria, along with other European countries, has been affected by cyber-attacks (eg, 'Bad Rabbit', 'WannaCry' and others) which targeted corporate networks. However, there is no publicly available information about initiated formal criminal proceedings with respect to these cyber-attacks or imposed penalties with final and binding court decisions.

Under the Bulgarian Penal Code, a number of information and data security violations qualify as criminal offences. Committing such an offence may be subject to imprisonment of one up to eight years and a fine of up to BGN10,000 (approximately EUR5,000). Under the established court practice, minor offences of this type have often been sanctioned with a fine in the region of BGN1,000 (approximately EUR500). In one serious computer crime and fraud offence, which affected more than 310 people and computers and caused damages of approximately EUR150,000, the offender was sentenced to imprisonment of two years.

Significant Private Litigation

Private litigation involving cybersecurity allegations or data security incidents or breaches includes court cases in which banks' clients have sought compensation for unauthorised payment transactions which occurred due to alleged an security breach of the servicing bank, as well as court cases in which natural persons have sought compensation for breach of data-privacy rights. Private litigation involving cybersecurity allegations is scarce, as the legal framework in the area of cybersecurity is relatively new.

6.10 Other Significant Issues

The undertakings providing public electronic communications networks and/or services under the ECA are required to ensure network security, provide for communications confidentiality and report any network incidents to the sector specific regulator – the Communications Regulatory Commission – in compliance with the specific regulations set forth in ECA. However, those undertakings are bound to fulfil the following obligations under the CA:

- when notified by the Chief Directorate Combating Organised Crime with the Ministry of Interior, immediately (if technically possible) to filter or terminate malicious internet traffic (which is the source of the cyber-attack) to the networks and information systems of the obliged entities;
- to co-operate with the National CSIRT for eliminating cyber-incidents identified in the networks or services of the respective undertakings providing public electronic communications networks and/or services; and
- when notified by the State Agency for National Security, immediately (if technically possible) to filter or terminate malicious internet traffic (which is the source of the

Djingov, Gouginski, Kyutchukov & Velichkov

10 Tsar Osvoboditel Blvd.
1000 Sofia, Bulgaria

Tel: +359 2 932 1100
Fax: +359 2 980 3586
Email: dgkv@dgkv.com
Web: www.dgkv.com

cyber-attack); this particular obligation applies only to entities designated as strategic objects (ie, in the telecoms sector in Bulgaria these are the three major mobile services-providers only – A1, Bulgarian Telecommunications Company and Telenor).