COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Bulgaria

TMT

Contributor

Boyanov & Co

Nikolay Zisov

Head of TMT Practice Group | n.zisov@boyanov.com

Ralitsa Nedkova

Principle Associate | r.nedkova@boyanov.com

Deyan Terziev

Senior Associate | d.terziev@boyanov.com

Teodora Peycheva

Junior Associate | t.peycheva@boyanov.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Bulgaria.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

BULGARIA
TMT

1. What is the regulatory regime for technology?

Technology in general is subject to various sectorial laws and regulations that govern different areas, such as: electronic communications, e-commerce, personal data, etc. More general legal provisions such as contract law, consumer protection and criminal law are also applicable to technology.

Besides the relevant EU directives and regulations the more specific local regulatory framework applicable to technology includes, among others:

- the Electronic Communications Act ("**ECA**");
- the Electronic Commerce Act which sets forth rules governing liability of internet service providers (i.e. access, caching and hosting providers);
- the Electronic Communications Networks and Physical Infrastructure Act;
- Regulation No. 1 of 22 July 2010 on the Rules for Use and Distribution and the Procedures for Primary and Secondary Allocation for Use, Reservation and Withdrawal of Numbers, Addresses and Names issued by the Chairman of the Communications Regulation Commission;
- General Terms for Carrying Out Public Electronic Communications, issued by the Chairman of the Communications Regulation Commission;
- Tariff of the Fees Collected by the CRC under the Electronic Communications Act;
- the Personal Data Protection Act;
- the Copyrights and Neighbouring Rights Act which is applicable to software and databases;
- the Bulgarian Criminal Code which regulates, inter alia, cybercrimes and technology–related offences.

2. Are communications networks or services regulated?

Yes, communications networks and services are regulated mainly by the Electronic Communications Act which currently to a large extent implements the existing European legal framework, e.g. the so-called Telecoms Package. The latest significant amendments introduced in December 2021 implemented Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

An "electronic communications network" is a totality of transmission systems, whether based on permanent infrastructure or centralized administrative capacity and, where applicable, switching or routing facilities and other resources, including network elements which are not active, permitting the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and TV broadcasting, and cable television networks, irrespective of the type of information conveyed.

An "electronic communications service" is defined as a service normally provided for remuneration, via electronic communications networks, which encompasses the following types of services: Internet access service; interpersonal communications service and services consisting wholly or mainly in the conveyance of signals, such as transmission services used for the provision of machine-to-machine and broadcasting services. The electronic communications service does not include services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.

3. If so, what activities are covered and what licences or authorisations are required?

Electronic communications for own needs through electronic communications networks without the use of a limited resource may be carried out freely.

The providers of publicly available [1] electronic communications service ("PECS") or publicly available electronic communications networks ("PECN") (see definitions in question 2) which do not use individually allocated scarce resource (e.g. numbers, radio frequencies, geostationary orbital position) are obliged to file a notification to the regulator about their intention to carry out such services. Notification is not required where number-independent interpersonal communications services are provided or access to a public electronic communications network is provided via a local radio network by undertakings, public sector organizations, non-governmental organizations or end-users for whom the provision of such access is not part of an economic activity or, is in addition to an economic activity or public service which is not dependent on the transmission of signals over such networks. An operator which has submitted a notification on carrying out public electronic communications shall comply with the general terms for performing such activities adopted by the Communications Regulation Commission.

Providers of PECN and/or PECS which need individually allocated radio frequencies or numbers from the National Numbering Plan or geostationary orbital position have to obtain an authorisation for use of individually assigned scarce resource from the regulator before commencing their activity. Authorisations are issued for initial period of up to 20 years, which can be further prolonged.

Authorisations are to be obtained following a special procedure commencing upon application of the operator. The application is in standard form and available on the website of the regulator (in Bulgarian only). In case the requested scarce resource is not sufficient for all applications then a tender procedure has to be organised and carried out by the regulator.

[1] ECS is deemed "publicly available" when available to the general public.

4. Is there any specific regulator for the provisions of communications-related services?

The main regulatory authority in matters of provision of communications-related services is the Communications Regulation Commission (in Bulgarian language "*Комисия за регулиране на съобщенията*"). The Communications Regulation Commission ("CRC") is responsible for regulation and control of the electronic communications services. Thus, the CRC ensures compliance with the primary and secondary national legal acts in the field of the electronic communications policy, the radio spectrum planning and allocation policy, and the postal services policy as well as compliance with EU regulations and policies by virtue of assignment of powers to the national competent authorities in the field of electronic communications.

When exercising its powers, the CRC may issue administrative acts – decisions and other regulatory legal acts as well as impose pecuniary sanctions to natural persons or legal entities who violated the provisions of the Bulgarian Electronic Communications Act and the other applicable legislative acts.

Also, the Council of Ministers, the National Radio Spectrum Council and the Minister of Transport, Information Technology and Communications have significant role in the regulation of communications-related services as they are responsible for exercising the state policy in the field of electronic communications.

5. Are they independent of the government control?

The Electronic Communications Act specifies that the CRC is an independent state authority which carries out regulatory and control functions in the field of electronic communications. The CRC is a collective state authority, which consists of five members, including a Chairperson and a Deputy Chairperson. The Chairperson of the CRC is designated and dismissed by decision of the Council of Ministers and appointed by order of the Prime Minister. Also, the Deputy Chairperson and two of the members of the CRC are elected and dismissed by a resolution of the National Assembly. One member of the CRC is appointed and dismissed by a decree of the President of the Republic of Bulgaria. All members of the CRC are elected and appointed upon open and transparent selection procedure. The term of office of the CRC's members, including the Chairperson and the Deputy Chairperson, is 5 years. A member of the CRC cannot serve for more than two full terms.

As mentioned above, each CRC member is elected by a different state authority – the Council of Ministers, the National Assembly or the President of the Republic of Bulgaria. Given this one may argue that in practice the CRC members might not always be completely independent.

6. Are platform providers (social media,

content sharing, information search engines) regulated?

Yes, different aspects of the services provided by platform operators are regulated in Bulgaria. Some regulations are established at EU level and are directly applicable in Bulgaria, other EU provisions are implemented at national level through local legislative acts and in some cases there are national specifications. Here is a non-exhaustive list of some of the main regulations which may be applicable to the platform providers depending on the situation:

i. **Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services ("Regulation (EU) 2019/1150") –** Regulation (EU) 2019/1150 (also known as "P2B Regulation") is directly applicable in Bulgaria to business users and corporate website users who provide or offer to provide online intermediation services and online search engines through which goods or services are offered to consumers or business users and corporate website users, established or residing in the EU, irrespective of the place of establishment or residence of the providers of those services and irrespective of the law otherwise applicable. The Regulation provides rules governing:
   - the relations associated with the online intermediation services and online search engines provided by the platform operators such as: rules regarding the restriction, suspension or termination of the online intermediation services provided to business users;
   - transparency of ranking which should be addressed in the terms and conditions of the platform provider;
   - any differentiated treatment afforded in relation to goods or services offered to consumers through and by the platform operators or by other business users/corporate website users that they control;
   - the requirements for providing a description of the type of ancillary goods and services which are offered and whether and under which conditions the business user is also allowed to offer its own ancillary goods and services through the online intermediation services.

ii. **Bulgarian E-commerce Act –**The Bulgarian E-commerce Act implements the provisions of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the Directive on electronic commerce). The Bulgarian E-commerce Act would be applicable in cases where the platform operators provide information society services. The Bulgarian E-commerce Act provides rules defining the requirements for providing the service recipients and the competent authorities general information about the service provider; rules regarding the storage of information in the terminal equipment of individuals and the access to such information (such as cookies); rules regarding the commercial communication; rules on provider's obligations upon conclusion of the contracts through electronic means; requirements for providing access to the general terms and the content of the contract, etc.

iii. **Bulgarian Consumer Protection Act –** Bulgarian Consumer Protection Act provides various provisions which protect the consumers' interest and it might be applicable where the platform providers render services to consumers. Inter alia, the Consumer Protection Act also governs the off-premises contracts and distance contracts which provisions might be applicable to certain services provided by the platform operators.

iv. **Bulgarian Act on the Supply of Digital Content and Digital Services and the Sale of Goods. –** The Act regulates the requirements concerning the contracts for the supply of digital content and digital services concluded between the sellers and the consumers, in particular the requirements concerning the conformity of the digital content or digital service, the consumer remedies in the event of failure to supply or lack of conformity of the digital content or digital service, the modalities for the exercise of those remedies, as well as the modification of the digital content or digital service. The Act also governs the sale of goods concluded between sellers and consumers, in particular the requirements concerning the conformity

of goods, the consumer remedies in the event of lack of conformity, the modalities for the exercise of those remedies and the commercial guarantees where the goods have digital elements such as movable items that incorporate, or are inter-connected with, digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions or other certain types of goods.

7. If so, does the reach of the regulator extend outside your jurisdiction?

In general, it is unlikely that the reach of the competent authorities would extend with respect to activities that take place outside Bulgaria, however there is no general rule that could be provided and each situation should be reviewed on a case-by-case basis and should be assessed individually.

8. Does a telecoms operator need to be domiciled in the country?

No, a telecoms operator does not need to be domiciled in Bulgaria, however it should designate a point of contact with the regulator.

9. Are there any restrictions on foreign ownership of telecoms operators?

No such general restrictions exist.

It should be noted that companies registered in jurisdictions with preferential tax treatment and persons controlled thereby are prohibited from direct or indirect participation in procedures for granting authorisation to an undertaking providing public electronic communication networks and/or services under the Electronic Communications Act, respectively acquisition of participation in such an undertaking, where the percentage of participation provides 10 or more than 10 per cent of the voting right in the general meeting of the legal entity.

10. Are there any regulations covering interconnection between operators?

Yes, operators shall have the right and, where requested by another operator – the obligation, to agree on interconnection of their networks for the provision of public electronic communications services and the ensuring of interoperability between services.

Operators shall be free to negotiate access and/or interconnection and enter into a written contract. The operators shall ensure access and/or interconnection in compliance with the obligations imposed by the Communications Regulation Commission (the “CRC”), where such have been determined.

The CRC shall encourage and, where necessary, impose on the undertakings providing public electronic communications networks and/or services, obligations for access and/or interconnection of services, with a view to promoting efficiency, sustainable competition, efficient investment and innovation, deploying very high-capacity networks and ensuring maximum benefit to end users.

As provided in the law, the CRC issues guidelines and publishes on its website the procedures applicable to access and interconnection to ensure that small and medium sized enterprises and operators with limited geographical coverage can benefit from the obligations imposed.

The terms and procedure for establishment of access and/or interconnection are contained in a regulation adopted by the CRC.

11. If so are these different for operators with market power?

The Communications Regulation Commission (“CRC”) may impose specific obligations on operators with significant market power (“SMP operators”) to provide efficient access and/or interconnection and interoperability of services to the benefit of end-users and to encourage efficient competition. These could be, inter alia, obligations for:

1. transparency (e.g. publication of specified information such as for example financial statements, prices, technical specifications, network characteristics and the expected development thereof, etc.);
2. non-discrimination;
3. accounting separation;
4. access to and use of necessary network elements and associated facilities;
5. price controls, including obligations relating to cost orientation;
6. access to physical infrastructure, buildings and physical infrastructure in buildings;
7. compliance with the terms on proposals of undertakings to make commitments on cooperation arrangements for co-investments

in new networks with very high capacity or for efficient and equitable access by third parties in the event of voluntary separation from a vertically integrated undertaking.

The CRC may impose, amend or revoke obligations in the case of:

1. voluntary separation from a vertically integrated undertaking;
2. migration from existing infrastructure;
3. proposals for co-investment commitments for the deployment of new networks with very high capacity in relation to the specific regulatory treatment of the new network elements;
4. only wholesale undertakings.

For achieving the purposes of the law, the CRC may, in exceptional cases, impose functional separation and other obligations for access and/or interconnection, with certain exceptions, after obtaining consent of the European Commission.

In certain cases specified in the law the CRC may require from an SMP operator to publish a reference offer with minimum content as per decision adopted by the CRC taking into account the applicable guidelines of the Body of European Regulators for Electronic Communications.

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

Customer terms and conditions for the provision of electronic communications networks and services are subject both to general consumer protection legislation (the Consumers Protection Act) and to sector-specific regulation and particularly to the Electronic Communications Act (the "ECA"), which defines the minimum content of such terms and conditions.

Pursuant to the ECA undertakings providing services to end-users are obliged to respect the principles of transparency and non-discrimination conforming to the type of technology used, the categories of subscribers, the traffic volume and the mode of payment, and to not allow advantages to specific end-users or group of end-users for the same services.

ECA determines which information operators have to make available to the consumers in the general terms and conditions ("GTC") or, respectively, individual contract in an explicit, comprehensive and easily accessible form. The minimum contractual information shall include, inter alia, information on all restrictions on the access and use of services and applications, the minimum level of service quality offered, as well as information on all procedures set up by the company for the measurement and control of data traffic.

Undertakings providing connection to PECN and/or PECS have to prepare GTC of their agreements with end-users in the cases where conclusion of individual contracts alone is practically inapplicable. The GTC are integral part of the individual contract between the ECS provider and the end-user and shall have a minimum mandatory content.

The operators shall elaborate and publish a price list of the services, stating prices of the services offered, price packages or tariffs and conditions for their use.

All conditions must be stated clearly, comprehensively and in a form easily accessible to subscribers.

Customers must be offered an initial duration of the contract that cannot exceed two years. The offered duration of contracts to customers may be up to one year. Regardless of the duration of the contract, the terms and procedures for termination of the contract may not be an obstacle to changing the undertaking providing the services.

A fixed-term contract may be extended solely with the express written consent of the subscriber regarding the conditions for extension. Where no such consent has been given, after expiry of the duration of any such contract it shall be transformed into an open-ended contract under the same conditions. The subscriber shall have a right to terminate the open-ended contract by a one month notice without any penalty and any agreements between the operator and the customer on the contrary shall be null and void.

13. What legal protections are offered in relation to the creators of computer software?

Computer programs are subject to copyright protection under the Bulgarian Copyright and Neighbouring Rights Act. Computer programs are protected as literary works and the protection applies to the expression of a computer program in any form. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright.

Bulgarian law does not provide for a copyright registration regime or any other administrative measures for the copyright to occur. Copyright arises automatically from the moment of creation of the work,

provided that the computer program is original, i.e. that it is the author's own intellectual creation and is fixed in tangible form. Business methods and computer programs as such are not patentable under Bulgarian law. Under certain circumstances computer-implemented inventions may be subject to patent protection if the patent claims show the presence of a technical effect.

As a general rule the copyright holder is the author, i.e. the natural person whose creative efforts have resulted in the creation of the respective work. However, as an exception from this rule, the Bulgarian Copyright and Neighbouring Rights Act provides that, unless agreed upon otherwise, copyright in computer programs and databases developed under an employment contract shall belong to the employer. This means that the copyright in software is acquired by the employer with the fact of creation of the software, i.e. it occurs automatically, by operation of law, and no additional steps for the transfer need to be completed.

14. Do you recognise specific intellectual property rights in respect of data/databases?

Yes, Bulgarian law recognises specific intellectual property rights in respect of databases. The copyright over databases in principle belongs to the person who has performed the selection and arrangement of the data. The Bulgarian Copyright and Neighbouring Rights Act grants also protection to the producers of databases – the natural persons or legal entities who have taken the initiative and the risk of investing in the collection, verification or use of the content of a database if this investment is substantial in quantitative or qualitative terms. The database producer has the specific (sui generis) right to prohibit the extraction by permanent or temporary transfer of the content of the database or essential part thereof in quantitative or qualitative terms on another medium in any way and in any form as well as the re-use (re-utilization) of the content of the database or a substantial part thereof in terms of quantity or quality by disclosure in any form, including distribution of copies, rental or provision by digital means. The specific right shall expire fifteen years counting from the first of January of the year following the date of completion of the database.

15. What key protections exist for personal data?

The main legislative act on personal data protection in the EU is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – the "GDPR") which became directly applicable in Bulgaria as of 25 May 2018. Rules supplementing the GDPR can be found in:

- the Personal Data Protection Act which ensures the effective enforcement of the GDPR by the local supervisory authority – the Bulgarian Commission on Personal Data Protection, contains a few locally-specific rules on data protection, and implements Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA;
- the Electronic Commerce Act which partially implements the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal d
- Privacy Directive"); it is important to point out that the consent requirement for cookies under Art. 5(3) of the e-Privacy Directive has not yet been properly transposed in Bulgarian law which is still relying on the previous opt-out regime that was made obsolete with the amendment of the e-Privacy Directive in 2009.
- the Electronic Communications Act which also implements texts of the e-Privacy Directive;
- sector-specific legislation (electronic communications, health, employment, gambling, private security, etc.).

In addition, guidelines on the application of the applicable rules are established by the European Data Protection Board and by the local Commission on Personal Data Protection.

Bulgarian law does not have significant deviations from the general EU-wide rules. As such, the processing of personal data must comply with the same basic rules and principles applicable within the EU: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, accuracy, integrity, confidentiality, accountability, privacy by design and by default. Processing is lawful when based

on one of the expressly listed legal grounds: consent, contractual necessity, legal obligation, legitimate interests, etc. with additional legal basis required for special categories of personal data. Data subjects may benefit from the rights to request access to and rectification or erasure of personal data, or restriction of processing, to object to processing, to withdraw their consent to processing, to data portability, and to lodge a complaint with a supervisory authority.

16. Are there restrictions on the transfer of personal data overseas?

There are no locally-specific rules for Bulgaria on the transfer of personal data overseas – the general legal regime of the GDPR applies.

Transfers of personal data to countries in the European Economic Area (the "EEA") are not restricted.

Transfers of personal data outside the EEA is generally permissible where the European Commission has decided that the respective third country ensures an adequate level of protection. Currently, the following countries have been recognized with an adequacy decision: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay.

In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The most commonly applied safeguards are contracts incorporating standard contractual clauses adopted by the European Commission, and group-wide binding corporate rules.

Transfer of personal data is also possible on the basis of the derogations provided for under the GDPR – for example, consent of the data subject, necessity for the performance of a contract with the data subject, necessity for the establishment, exercise or defence of legal claims, etc.

As a result of the "Schrems II" decision of the Court of Justice of the European Union, it was determined that the safeguards for transfer of personal data are not sufficient to guarantee an adequate level of protection for personal data, and supplementary measures may need to be implemented (encryption, pseudonymization, etc.). Controllers are expected to perform transfer impact assessments in order to determine the permissibility of data transfers to third countries and the measures that need to be adopted to supplement the relevant safeguards in this regard. The European Data Protection Board has issued Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, as well as Recommendations 02/2020 on the European Essential Guarantees for surveillance measures in which the topic is examined in great detail.

17. What is the maximum fine that can be applied for breach of data protection laws?

The maximum fines for violating the applicable data protection rules according to the GDPR are up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

18. What additional protections have been implemented, over and above the GDPR requirements?

The Bulgarian Personal Data Protection Act complements the GDPR where it was permitted for additional protection or specific conditions for processing of personal data to be implemented at local level. Without providing an exhaustive list, notable examples are:

- The age of consent for children in the context of offering information society services is set to 14.
- A data controller or processor may copy an identity document, a motor vehicle driving license or a residence document only if this is provided for by law.
- Open public access to any information containing a personal identification number or a foreigner personal number shall not be provided unless otherwise provided for by 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 relevant service is provided.
- The retention period for job applicant personal data cannot exceed 6 months without the data subjects consent.

Apart from the Personal Data Protection Act, there are a number of sector specific laws that contain rules on personal data protection (electronic communications,

electronic commerce, consumer protection, healthcare, gambling, finance, private security, etc.).

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

As a general comment, and without discussing the implications of GDPR which is directly applicable in Bulgaria, there is no specific regulation and there are no general requirements under Bulgarian law for use of cloud-based services. There are however certain specific conditions and requirements for the use of cloud – based services applicable to certain types of data and certain industry sectors. Thus, for instance, there would be regulatory difficulties related to the usage of a cloud service for storage of information classified as state secret, and it would be impossible to do so with respect to data classified as "*Top Secret*". Also, under Bulgarian law, the bank supervision authorities have quite broad powers to request and collect information from financial institutions, including to perform on-site inspections. They have the right of free access to all IT systems and offices of the financial institutions. Those inspection rights extend also to the subcontractors and service providers, including providers of cloud-based services.

Operators of essential services and key digital service providers, such as search engines, cloud computing services and online marketplaces have to comply with the security and notification requirements under the Cybersecurity Act adopted in 2018. The Cybersecurity Act and the respective secondary acts fully implement, with minimum derogations, the Directive on Security Network and Information Systems (Directive (EU) 2016/1148) ('the NIS Directive').

20. Are there specific requirements for the validity of an electronic signature?

In Bulgaria, electronic signatures are regulated by Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS") and the Electronic Document and Electronic Trust Services Act (last amended in 2020, "EDETSA"). Specific rules on the usage of e-signatures in the employment context are contained in Ordinance on the type and requirements for the creation and storage of electronic documents in the employment file of the employee.

eIDAS contains the definitions and requirements for the three types of electronic signatures – simple, advanced and qualified. All three types of electronic signatures are recognized in Bulgaria.

EDETSA specifies the types of transactions and documents that cannot be established in electronic form where the use of electronic signatures is not permitted:

i. When the law mandates the observance of a qualified written form:
    - Contracts to sell, purchase or establish in rem rights over real property;
    - Contracts to sell or purchase motor vehicles or boats;
    - Contracts for sale and purchase of a decedent's estate;
    - Mortgage contracts;
    - Transfer and pledging of a claim secured by mortgage, the assumption of such a claim and the imposition of an attachment on it, as well as its novation and substitution in obligation;
    - Donation contracts;
    - Contracts for transfer or pledge of an enterprise as a going concern;
    - Contracts for transfer or pledge of shares in a limited liability company;
    - Consent for deletion of a mortgage from the Real Estate Registry;
    - Powers of attorney for transactions where a notary deed or a certification by notary is required;
    - Powers of attorney for a procurator or for a commercial representative.
    - Power of attorney for withdrawal of sums from a money deposit;
    - Various corporate procedural steps and transactions (most notably transfer of shares in a limited liability company, transfer of a business as a going concern, etc.);
    - Handwritten or notarial will.
ii. When the act of physical possession of a document has legal significance:
    - Transfer or pledge of physical registered shares;
    - Transactions involving certain types of materialised securities (e.g. promissory note, bill of exchange, cheque).

The specific rules on e-signatures in employment law are related to the creation of documents that form part of

the employment file for each employee – it contains all documents in connection with the establishment, existence, modification, and termination of the employment relationship (e.g. employment contract, termination notice, etc.). In cases where electronic employment documents are signed by the employer, this must be done with a qualified electronic signature. There are significant organisational (implementation of certain internal procedures, consent of the employee) and technical requirements for the creation and/or storage of electronic documents in the employment file, such as: two-factor authentication, specific log requirements, usage of electronic registered delivery service, etc., which are often problematic to implement in practice.

eIDAS provides that an e-signature shall not be denied legal effect and admissibility in legal proceedings solely because it is in electronic form. However, the legal effect given to different types of e-signatures in court proceedings is left to the national law of EU Member States. The only exception is that a qualified electronic signature must be given the same legal weight as a handwritten signature.

Article 13(4) of the EDETSA further specifies that the legal effect of advanced and simple electronic signatures could also be equivalent to handwritten signatures, if this is agreed between the parties to a contract. This approach is highly recommended in Bulgaria as it provides additional safety in future litigation – otherwise, the courts could refuse to acknowledge that the document was signed at all which could lead to an unfavourable transfer of the burden of proof. The court will weigh all evidence in the case and the arguments of the parties.

A document signed with a qualified electronic signature, or with a simple / advanced electronic signature where an agreement was reached as per Article 13(4) of the EDETSA, is likely to be accepted as evidence, i.e. such documents would be considered as proof that the statements included

in them were made by the person indicated as signatory. Such documents are generally enforced by Bulgarian courts, unless the counterparty contests successfully their content and/or signature.

In Bulgaria, the supervisory body for qualified trust service providers is the Communications Regulation Commission. The national trust list maintained by the CRC can be consulted at the following address: https://crc.bg/files/_en/TSL_BG.pdf

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

Not necessarily. The transfer of assets or third-party contracts would usually require an express contract, while in certain scenarios the transfer of employees might occur by operation of law. Notably, these would be the cases where the outsourcing supplier also takes over the outsourced activity, including certain material assets pertaining thereto or autonomous part of the assignor's undertaking which includes the respective activity and employees. In these cases the employment relationship shall not be terminated but all rights and obligations of the transferring enterprise prior to the change arising from employment relationships existing as of the date of the transfer shall be transferred to the acquiring enterprise.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

At this point under Bulgarian law there is no specific regulation of the legal liability arising from AI malfunctioning. The *Concept for Development of the Artificial Intelligence in Bulgaria until 2030* adopted by the Bulgarian Government in December 2020 outlines that large part of the existing EU legislation on product safety and liability, including specific sectoral rules complemented by the relevant national laws, covers new AI applications and may apply to them.

Given this, at this point and absent any specific statutory rules governing the legal liability arising from AI acts and processes, it may be concluded that in case of AI malfunctioning the general civil contractual and tort law rules as well as the consumer protection rules (where appropriate) would apply. In extreme cases the administrative and criminal liability of the responsible persons may also be engaged.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

(a) The Bulgarian Cybersecurity Act adopted in 2018 sets out substantive rules with regards to cybersecurity, defines both the scope of entities, which are subject to the obligations contained therein, and the authorities which must observe compliance with its rules. Furthermore, the Cybersecurity Act sets out a number of technical and organisational measures, which must be

adopted by the entities that are subject to its regulation.

Bulgaria has also adopted secondary legislation which aims to facilitate the implementation of the Cybersecurity Act, namely – the Ordinance on Minimal Requirements for Network and Information Security.

The Cybersecurity Act and the respective secondary acts fully implement, with minimum derogations, the NIS Directive.

(b) Acts of hacking / DDOS attacks could qualify as computer crimes under the Bulgarian Criminal Code (Chapter 9”a”).

24. What technology development will create the most legal change in your jurisdiction?

Developments in the field of artificial intelligence bring forth hard to answer questions concerning liability for damages, product safety, intellectual property, personal data protection, and traffic regulation. These legal challenges would require a significant overhaul of the current legislative framework.

25. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

Most legislation that has an impact on the development and commercialization of innovative technological solutions in Bulgaria is adopted at EU level. Businesses have often expressed their concerns regarding potential overregulation which could impede progress in the EU compared to other parts of the world. Such concerns have been recently expressed in view of the proposal for an EU Regulation on Artificial Intelligence which raises a high bar for the development and implementation of certain AI technologies to the extent that it may potentially have a stifling effect on innovation within the Union.

Another recent example is the reform of the personal data protection legal framework in 2018 with the GDPR, the ECJ judgment on the “Schrems II” case and the related recommendations of the European Data Protection Board which introduced significant (often impossible to implement in practice) requirements for personal data transfers from the EU to the United States and other “high-risk” third countries.

26. Do you believe your legal system specifically encourages or hinders digital services?

Digital services are overall governed at EU level. The Bulgarian legal system does not deviate significantly from the EU rules in a manner that would specifically encourage or hinder digital services.

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

The Bulgarian legal system currently does not specifically regulate the usage of artificial intelligence. As such, significant legislative changes would be necessary to address the complex legal issues related to the development and implementation of such technologies.

Contributors

Nikolay Zisov
Head of TMT Practice Group
n.zisov@boyanov.com

Ralitsa Nedkova
Principle Associate
r.nedkova@boyanov.com

Deyan Terziev
Senior Associate
d.terziev@boyanov.com

Teodora Peycheva
Junior Associate
t.peycheva@boyanov.com