The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Bulgaria: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection and cyber security laws and regulations that may occur in Bulgaria.

This Q&A is part of the global guide to Data Protection & Cyber Security. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/practice-areas/data-protection-cyber-security/

Dimitrov, Petrov & Co.

Country Author: Dimitrov, Petrov & Co

The Legal 500

Desislava Krusteva, Partner

desislava.krusteva@dpc.bg

The Legal 500

Gavrail Poterov, Associate

gavrail.poterov@dpc.bg

Svilena Rakshieva, Associate

svilena.rakshieva@dpc.bg

1. **Please provide an overview of the legal framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the laws enforced)?**

(i) General Laws

The main legislative act that governs the privacy in Bulgaria is the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). In addition, the Personal Data Protection Act (in Bularian: Закон за защита на личните данни) (PDPA) regulates some specific aspects of the processing of personal data with GDPR derocations and transposes Directive (EU) 2016/680. With the latest amendment on 26 February 2019, the PDPA, which originally took effect in 2002, has been synchronised with the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). The supervisory authority in charge of performing tasks and exercising powers under the GDPR and the PDPA is the Commission for Personal Data Protection (CPDP).

Finally, it should be noted that the right to privacy is also a constitutional right recognized and protected by the Constitution of the Republic of Bulgaria.

(i) Sectoral Laws

In Bulgaria, there are a few sectoral laws that regulate the collection and use of personal data:

- The E-Commerce Act
  - transposes the rules on the use of cookies of the EU E-Privacy Directive (Directive 2002/58/EC) and thus, regulates the regime when providers of information society services may store information or receive access to information stored in the terminal device of the service recipient

- the CPDP is the supervisory authotity when it comes to the processing of personal data stored in the terminal device of the service recipient (e.g. through the use of cookies).

- The E-Communications Act
  - transposes the E-Privacy Directive, and regulates the regime on how public electronic communication service and network providers process users' personal data when providing public electronic communication services and networks (e. g. traffic data, location data, etc.);
  - Commission fot Regulation of Communications is the main supervisory authority under this law, but the CPDP performs tasks and exercises specific powers under the Electronic Communications Act in addition to those under the GDPR and the PDPA with regard to the processing of personal data of users of public electronic communication service and network such as traffic data.

- The Law on Credit Institutions (LCI)
  - regulates bank secrecy
  - the Bulgarian National Bank supervises the compliance with the provisions regarding bank secrecy.

- The Ordinance No 22 of 16 July 2009 on the Central Credit Register
  - regulates the operation of, provision to and receipt of credit information from the Bulgarian Central Credit Register
  - the Bulgarian National Bank supervises the compliance with the provisions regarding the provision and use of information from the Central Credit Register.

- The Health Act (HA)
  - regulates the collection, processing, use, storage and provision of medical information and documentation
  - the Executive Agency 'Medical Audit' at the Ministry of Health supervises the compliance with the provisions collection, processing, use, storage and provision of medical information and documentation.

- The Criminal Code (CC)
  - governs cybercrimes such as the disclosure of personal data through unlawful distribution of computer programs, passwords, codes or other similar data for access to information systems.

2. **Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements?**

Are there any exemptions?

The GDPR removed the general obligation to notify the regulatory authority before processing personal data. No such general notification obligation to notify has been adopted under national law.

According to Article 25b PDPA both controllers and processors are obliged to notify the CPDP with specific details about an appointed data protection officer (DPO), including the DPO's: name, national personal identification number and contact details, if they appoint DPO.

3. **How do these laws define personally identifiable information (PII) versus sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?**

   All the key definitions related to data protection and privacy are set forth in GDPR. The definition of personally identifiable information (PII) stems from the definition of personal data, which is data relating to an identified or identifiable natural person (Article 4(1) GDPR). An identifiable natural person is one who can be identified directly or indirectly by reference to:

   - An identifier, such as a name;
   - An identification number;
   - Location data;
   - An online identifier, such as an internet protocol (IP) address;

- One or more factors specific to the person’s physical, physiological, genetic, mental, economic, cultural, or social identity.

As personal data is also considered information relating an identified or identifiable natural person that have undergone pseudonymization, since pseudonymised data could still be attributed to a natural person with the use of additional information (Recital 26 GDPR; for more information on pseudonymised data, see Practice Note, Anonymization and Pseudonymization Under the GDPR (W-007-4624).

Sensitive PII relates the special categories of personal data as defined to Article 9, para. 1 GDPR, namely data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or relating to trade union membership, genetic or biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation.

The PDPA provides for some specific definitions, incl.

- ‘processing on a large scale’ is monitoring and/or processing of personal data of a significant or unlimited number of data subjects or volume of personal data in cases where the main activities of the data controller or the data processor of personal data, including the means for their execution, consist in such operations (para. 1, it. 15 of the Addition provisions of the PDPA);
- ‘public body’ is a state or local authority or structure, the main purpose of which is related to the spending of public funds.

4. **Are there any restrictions on, or principles related to, the**

general processing of PII – for example, must a covered entity establish a legal basis for processing PII in your jurisdiction or must PII only be kept for a certain period? Please outline any such restrictions or "fair information practice principles" in detail?

(i) In Bulgaria, controllers and processors must process personal data in accordance with the principles set out in GDPR:

- Lawfulness, fairness, and transparency – the personal data must be processed fairly, lawfully, and in a transparent manner. This means that for any processing of PII there should be legal basis, otherwise the processing would be unlawful. (see below)
- Purpose limitation – the personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Data minimisation – the personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accuracy – the personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Storage limitation – the personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Integrity and confidentiality – the personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- Accountability – the controller shall be responsible for, and be able to demonstrate compliance with all the above-listed principles.

(ii) In particular, one of the legal bases for processing as per Article 6 GDPR must be satisfied in order for the processing of personal data to be lawful:

- Data subject (the concerned natural person) has granted his/her consent; OR
- If processing of personal data is necessary:
  - For the performance of a contract to which the data subject is a party or to take steps at the data subject's request prior to entering into a contract.; OR
  - For compliance with a legal obligation to which the controller is subject; OR
  - To protect the vital interests of the data subject or another natural person. 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 purposes of the controller's or a third party's legitimate interests, except if the data subject's interests or fundamental rights and freedoms override the controller's interests, especially if the data subject is a child.

5. **Are there any circumstances where consent is required or typically used in connection with the general processing of PII and, if so, are there are rules relating to the form, content and administration of such consent?**

   The PDPA introduces certain instances in which the consent is required:

   - According to Article 25k PDPA consent is required in the context of personnel recruitment in cases where the employer wishes to store, and process submitted job applications for a period longer than 6 months as from the end of the respective current recruitment procedure (for instance, for the purposes of future recruitment procedures).
   - Pursuant to Article 25c PDPA the consent of a parent or guardian exercising parental rights must be obtained whenever personal data of a minor under the age of 14 is processed on the basis of consent. This requirement applies not only in the context of information society services, but to any form of processing of such data based on consent.

   In any case data subject's consent must be:

   - Freely given,meaning the data subject has a genuine or free choice and is able to refuse or withdraw consent without detriment
   - Specific, meaning that consent should cover all processing activities carried out for the same purpose or purposes, but when the processing has multiple purposes, consent

should be given for each of them

- Informed, meaning the data subject should be informed on the controller's identity and the purposes of the processing
- Unambiguous.

The consent could be withdrawn at any time and in such case the controller must stop the processing of personal data.
Consent may be provided by:

- A written or oral statement
- Electronic means, such as ticking a box when visiting a website or choosing technical settings for information society services, so long as the request is clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided.
- Another statement or conduct that clearly indicates the data subject's acceptance of the proposed processing. Silence, pre-ticked boxes, or inactivity does not constitute valid consent. (Article 7 and Recitals 32 and 42 GDPR).

6. **What special requirements, if any, are required for processing sensitive PII? Are there any categories of PII that are prohibited from collection?**

The rules of the GDPR with regard to processing of special categories of personal data apply. No special national rules have been adopted in this regard. According to Article 9, para. 2 GDPR, processing of special categories of personal data is prohibited unless one of the following applies:

- The data subject has given explicit consent to the processing for one or more specified purposes unless EU or member state law prevents the data subject from lifting the general prohibition on this sort of processing.
- The processing is:
  - necessary to carry out the obligations or exercise the specific rights of the controller or

data subject in the field of employment, social security, or social protection law; and
- EU or member state law or a collective bargaining agreement authorises the processing and provides for appropriate safeguards for the data subject's fundamental rights and interests.

- The processing is necessary to protect the vital interests of the data subject or of another natural person when the data subject is physically or legally incapable of giving consent.
- A foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim carries out the processing in the course of its legitimate activities with appropriate safeguards and:
  - the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and
  - the data is not disclosed outside the body without the data subject's consent.
- The processing relates to personal data that the data subject has manifestly made public.
- The processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest on the basis of EU or member state law and:
  - is proportionate to the aim pursued
  - respects the data protection rights, and
  - provides for suitable and specific measures to safeguard the data subject's fundamental rights and interests.
- The processing is necessary for one of the following purposes and subject to the specific safeguards:
  - preventative or occupational medicine
  - the assessment of an employee's working capacity
  - medical diagnosis, or
  - the provision of health or social care or treatment or the management of health or social care systems and services.
- The processing is necessary for public health reasons, such as protecting against serious cross-border health threats or ensuring high standards of quality and safety of health care, medicinal products, or medical devices, on the basis of EU or member state law, including professional secrecy, which provides suitable and specific measures to safeguard the data subject's rights and freedoms.
- The processing:
  - is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, and is based on EU or member state law is proportionate to the aim pursued, respects data protection rights, and provides for suitable and specific

measures to safeguard the data subject's fundamental rights and interests.

The processing of personal data relating to criminal convictions and offences or related security measures must be carried out only under an official authority's control or when EU or member state law authorises it and provides for appropriate safeguards for the data subjects' rights and freedoms (Article 10 GDPR). In any other circumstance the processing of such personal data is prohibited.

7. **How do the laws in your jurisdiction address children’s PII?**

   Personal data of children are being treated as any other personal personal data in accordance with the requirements of the GDPR. However, a special attention should be paid whenever such personal data are prosessed since childred are more vulnerable data subjects and this affects the risks related to such processing.

   As for the requirement under Article 25c PDPA to obtain a parent or guardian exercising parental rights whenever for processing the personal data of a minor under the age of 14 based on consent, please refer to Question 5.

8. **Are owners or processors of PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so,**

please describe how businesses typically meet these requirements.

The obligations under Article 30 GPDR pursuant to which data controllers and data processors are obliged to keep and regularly update record of all their data processing activities, are fully applicable. So are GDPR requirements of Article 24, 29 and 32 relating to the obligation of data controllers and data processors to introduce appropriate technical and organization measures for data protection and to implement respective internal rules/ instructions.

Additionally to the above requirements, the PDPA introduces the following rules:

- Pursuant to Article 25i PDPA, the employer, acting in the capacity of data controller, is held to implement comprehensive rules and procedures, and to inform the employees accordingly, in case the following practices are implemented within the employer's organization:
  - whistleblowing systems;
  - restrictions on the use of business resources;
  - systems for access control and of control of the working time and the work discipline.

These rules and procedures should contain provisions on the scope, the responsibilities and the methods used for imposing the above practices. The documents should be established taking into account the business activity of the employer and should not restrict data subjects' rights.

In addition, data controllers and data processors are required to adopt and apply rules which introduce appropriate technical and organizational measures to protect the rights and freedoms

of data subjects in case of large-scale processing of personal data or of systematically large-scale surveillance of publicly accessible areas, including through CCTV. The rules for systematically large-scale surveillance of publicly accessible areas should contain the legal bases and purposes of the processing, the territorial scope of the surveillance and the means of the monitoring, the records' storage period and deletion, the right of access of the monitored persons, as well as restrictions on the access to the information by third parties, and should inform the public on the surveillance carried out (Article 25e PDPA).

Since the above requirements were introduced into national legislation recently (following the promulgation of the new Bulgarian PDPA of end February 2019), there are no clearly established business practices demonstrating how businesses typically meet it. In general, a set of written documents - registers (records) and internal rules, have to be in place and regularly updated.

9. **Are consultations with regulators recommended or required in your jurisdiction and in what circumstances?**

In accordance with Article 36, para. 1 GDPR the data controller is required to consult the data protection authority (DPA) prior to the processing, in cases where the performed data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the

risk. In addition, the PDPA implements the possibility left for Member States under Article 36, para. 5 GDPR and requires that prior consultation takes place when personal data are processed through the performance of a task in the public interest, including in relation to social protection and public health (Article 12, para. 2 PDPA). The prior consultation is performed pursuant to the procedures under Article 36, para. 2 and 3 GDPR.

10. **Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?**

No special national rules have been adopted with regard to conducting risk assesments. The general requirements with regard to the performance of Data Proection Impact Assessments (DPIA) of Article 35 GDPR apply.

Data controllers are responsible for introducing appropriate safeguards to ensure compliance with the GDPR taking into account the risks of various likelihood and severity to the rights and freedoms of natural persons‘ (Article 35, para. 1 GDPR).

On 13.02.2019, the CPDP published on its website a list of the types of processing operations for which DPIA is required in accordance with Article 35, para. 4 GDPR. Pursuant to this list, data controllers whose main or single establishment is on the territory of the

Republic of Bulgaria are required to conduct compulsory DPIA in each of the following cases:

- Large scale processing of biometric data for the purposes of the unique identification of a natural person, which is not occasional;
- Processing of genetic data for profiling purposes which produces legal effects for the data subject or similarly significantly affects them;
- Processing of location data for profiling purposes which produces legal effects for the data subject or similarly significantly affects them;v
- Processing operations for which the provision of information to the data subject pursuant to Article 14 of GDPR is impossible or would involve disproportionate effort or is likely to render impossible or seriously impair the achievement of the objectives of that processing, when this is related to large scale processing;
- Personal data processing by controller whose main place of establishment is outside the EU when its designated representative for the EU is located on the territory of the Republic of Bulgaria;
- Regular and systematic processing for which the provision of information pursuant to Article 19 GDPR by the controller to the data subject is impossible or involves disproportionate efforts;
- Processing of personal data of children in relation to the offer of information society services directly to a child;
- Migration of data from existing to new technologies when this is related to large scale data processing.

Article 35, para. 7 GDPR sets out the minimum features of a DPIA, namely:

- a systematic description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks and demonstrate compliance with the Regulation.

11. **Do the laws in your jurisdiction require appointment of a data protection officer, or other person to be in charge of privacy or data protection at the organization? What are the data protection officer's legal responsibilities?**

GDPR rules and requirements with respect to the appointment of a data protection office fully apply.

When the appointment of a data protection officer is required or when the company has, without having the obligation, decided to appoint a data protection officer, the appointment shall be notified to the Bulgarian Commission for Personal Data Protection. The notification includes names, national personal identification number/ personal identification number of a foreigner, and contact details.

The data protection officer's legal responsibilities are entirely covered by GDPR provisions (Article 37 GDPR and following) and Bulgarian legislation does not go beyond these provisions.

12. **Do the laws in your jurisdiction require providing notice to individuals of the business' processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).**

Data subjects' information rights, outlined in the GDPR, fully apply in Bulgaria. No special national rules have been adopted in this regard.

Pursuant to the provisions of Article 13 and 14 GDPR, data controllers shall duly inform data subjects on activities involving processing of their personal data. The information notice must include:

- identification of the company – data controller: title and contact details, including contact details of the company's data protection officer, if such is appointed (address, e-mail, telephone, etc.);
- the categories of personal data processed and the purposes of the processing;
- the categories of recipients of personal data outside the company, and whether data will be transferred to third countries, outside the EU;
- the storage periods;
- information on data subjects' rights and on how they can be exercised;
- information on data subjects' right to lodge a complaint with the national data protection authority;
- whether the provision of personal data is a statutory or contractual requirement, as well as the possible consequences if data are not provided;
- (if applicable) whether the company performs automated decision making, including profiling.

In addition to the above, pursuant to the provisions of the PDPA (Article 25e and 25i PDPA) data controllers (the employers) shall inform data subjects (the employees) in case the following practices are implemented and carried out within the company:

- whistleblowing systems;
- restrictions on the use of business resources;
- systems for access control and of control of the working time and the work discipline.
- videosurveillance.

The controller is responsible to make sure that the concerned are

informed about the content of the information notice without specific requirement on how to inform them. It is, however, both in the interest of and an obligation for the controller to be able to prove the compliance with its information obligation. In its ’10 Practical Steps on the Application of the GDPR’ guidance document, the Bulgarian PDPC suggests that information notices may be brought to the attention of data subjects through the website of the respective company, or by other suitable means available to the data subjects.

13. **Do the laws in your jurisdiction apply directly to service providers that process PII, or do they typically only apply through flow-down contractual requirements from the owners?**

GDPR as well the PDPA apply directly to both the owner of PII (the data controller) and the service providers that process PII, irrespective of whether the latter process the PII on behalf of the owner (as data processors) or for their own purposes (as data controllers).

When service providers act as data processors (and process PII solely on bahalf of the owner and under the latter’s instructions), the relations between them and the owner have to be arranged by a written contract or other written and binding legal act, containing and setting up the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the rights and obligations of

both parties (Article 28 GDPR).

Notwithstanding the obligation to settle controller-processor relations in writing, both GDPR and the PDPA contain provisions which directly apply to data processors, such as the obligation to observe the general principles for data processing, to keep records of data processing activities, to implement appropriate technical and organisational measures to ensure an adequate level of data security, etc.

14. **Do the laws in your jurisdiction require minimum contract terms with service providers or are there any other restrictions relating to the appointment of service providers (e.g. due diligence or privacy and security assessments)?**

No special national rules have been adopted with regard to minimum contract terms with service providers or any other restrictions relating to the appointment of service providers have been adopted.

The general requirements with regard to engaging data processors in accordance with Article 28 GDPR apply:

- Controllers may only use processors that guarantee they will implement appropriate technical and organisational measures to protect data subjects' rights.
- Processors must not engage another processor without the controller's specific or general written authorisation. If the processor wants to add or replace other processors, it must first give the controller an opportunity to object to the changes.

- Processors must also have a contract or another legal agreement with the controller that, with regards to processing, sets out:
  - The subject matter and duration
  - The nature and purpose
  - The type of personal data and categories of data subjects
  - The controller's obligations and rights
- The written contract or legal agreement may be in electronic form and specify that the processor:
  - Will only process personal data on the controller's documented instructions; or if EU or member state law requires it and the processor informs the controller about the legal requirement before processing unless the public interest prohibits this disclosure
  - Ensures that authorised persons have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
  - Has taken required security measures
  - Respects the conditions for engaging another processor
  - Can fulfil the controller's obligation to respond to requests for exercising data subjects' rights
  - Assists the controller in ensuring compliance its obligations under Articles 32 to 36, GDPR, including:
  • implementing security measures to protect processing
  • notifying a personal data breach to the supervisory authority
  • communicating personal data breaches to the data subject
  • carrying out data protection impact assessments, and
  • consulting the supervisory authority prior to processing if the data protection impact assessment indicates this is required.
  - Deletes or returns all personal data to the controller at the end of the provision of processing services, at the controller's discretion and deletes existing copies unless EU or member state law prevents this
  - Makes available all information necessary for the controller to demonstrate compliance, including allowing for and contributing to audits.

15. **Is the transfer of PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (for example, does cross-border transfer of PII require notification to or authorization form a regulator?)**

The general requirements with regard to transfers of personal data

according to the GDPR apply. The free movement of personal data within the EU is neither restricted nor prohibited (Article 1, para. 3 GDPR).

The GDPR restricts transfers of personal data outside the EU. It allows for transfers outside the EU to third countries or international organisations in compliance with certain conditions set out in Articles 44 to 50. These conditions allow for transfers:

- On the basis of an EU adequacy decision (Article 45 GDPR)
- Subject to appropriate safeguards (Article 46, GDPR)
- Under binding corporate rules (Article 47 GDPR)
- Under approved codes of conduct and certification mechanisms (Article 40 GDPR)
- If based on an international agreement, such as a mutual legal assistance treaty (Article 48 GDPR)
- Under a specific derogation (Article 49 GDPR), such as:
  - transfers due to important reasons of public interest;
  - transfers qualified as not repetitive and that only concern a limited number of data subjects
  - transfers necessary for the establishment, exercise, or defence of legal claims
  - non-repetitive transfers involving personal data related to only a limited number of data subjects
- Under international cooperation mechanisms (Article 50 GDPR).

No additional national rules have been adopted with regard to transfers of personal data outside Bulgaria. Cross-border transfers of PII do not require notification to or authorization form the CPDP.

Currently, the most commonly used instrument/ safeguard for lawfully transfering personal data outside EU are the EU standard

data protection clauses (Art. 46, para. 2, item ‘c’ GDPR). However, it really depend on the specific data transfer which instrument is the most appropriate one.

16. **What security obligations are imposed on PII owners and on service providers, if any, in your jurisdiction?**

GDPR requires PII owners to ensure that they process personal data in a manner that provides an adequate level of data security. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5 (f) GDPR).

When implementing appropriate technical or organisational measures, controllers and processors must consider the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing against the risks to the data subjects’ rights and freedoms. When choosing appropriate measures, the following are considered:

- Pseudonymisation and encryption of personal data
- Ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing, and evaluating the

measures' effectiveness for ensuring secure processing
- The ability to ensure that any personel of the controller or processor that has access to personal data does not process them except: on the controller's instructions; or if EU or member state law requires the processing (Article 32 GDPR).

The above security obligations fully apply in Bulgaria. In addition to GDPR requirements, the PDPA introduces the following security-related specific rules:

- Pursuant to Article 25g, para. 2 PDPA data controllers providing electronic services shall take appropriate technical and organisational measures which prevent the national personal identification number/ the personal identification number of a foreigner from being the only means of identifying the user when providing remote access to the service.

With the entry into effect of the GDPR the Bulgarian Ordinance No 1 of 30 January 2013 on the Minimum Level of Technical and Organizational Measures and the Admissible Type of Personal Data Protection (Ordinance No 1) was repealed. The Bulgarian CPDP has announced that it will issue a soft-law instrument (Metodical Guidelines) replacing the Ordinance No 1 but the exact time when this will happen remains unknown.

17. **Does your jurisdiction impose requirements of data protection by design or default?**

GDPR applies directly. There are no local specific requirements within the Bulgarian data protection legislation in relation to the data protection 'by design' and 'by default' concepts. Data

controllers are thus required to undertake data protection measures at the design stage, as well as to ensure these measures by default. With respect to the data protection ‘by design’ data controllers are obliged to introduce and implement both at the time of the determination of the means for processing and at the time of the processing itself, appropriate technical and organisational measures, designed to implement data protection principles (Article 25, para. 1 GDPR). Regarding data protection ‘by default’, data controllers have to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed (Article 25, para. 2 GDPR).

18. **Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?**

(i) All the provisions of GDPR regarding personal data breaches directly apply. Under Article 4, para 12 GDPR, a ‘personal data breach’ is a 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.

(ii) The Cybersecurity Act (CA)

The CA implementing the NIS Directive (Directive (EU) 2016/1148) imposes obligations to implement diverse measures to ensure proper network and information security on the a very wide range of

addressees such as administrative authorities; operators of essential services operating in the sectors: energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure; digital service providers providing services such as online marketplace, online search engine, cloud computing services; other organisations providing public services and persons exercising public functions. Enterprises that are micro and small digital service providers, within the meaning of the Bulgarian Micro and Small Enterprises Act, are among the entities, that are excluded from the scope of the CA.

The CA does not have a definition for ‘security breach’ but includes definitions about events related to security breaches such as:

- ‘Cyber attack’ - an attempt to destroy, disclose, modify, prohibit, steal or obtain unauthorized access to / unauthorized use of an information asset
- ‘Cyber threat’ - the possibility of malicious attempts to break or interrupt the computer network, system, services, and data
- ‘Cyber incident’ - an event or a series of unintended or unexpected cybersecurity events that are likely to cause compromisation of activities and threaten the security of the information.

(iii) There are also many **sectoral laws** which address security breaches most important of which are:

- E-Communications Act
  - Appendix No. 4 to General requirements of the Communications Regulations Commission (CRC) in the implementation of public electronic communications defines the types of ‘breach of security or integrity, which has significant impacted on the functioning of the networks or services’ in five categories:
- human error - incidents caused by internal personnel, including through incorrect configuration or incorrect deployment of network facilities, platforms, program

applications, archives and databases, and misuse of network resource and incident management procedures;

- failures in the technical and software provision;
- natural disasters - including severe weather conditions, floods, fires, earthquakes, landslides, etc .;
- malicious attacks - acquiring unauthorized physical or logical access to networks, systems, applications, data, or other information resources from individuals or software that may result from targeted internal or external attacks;
- external causes - includes human errors, incorrect procedures and damage caused by other countries.

Whether the breach has 'significantly impacted on the functioning of the networks or services' is being determined by further criteria based on the 'duration of the impact' and 'amount of impacted users'.

- The E-Communications Act defines 'personal data breach' as a 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 in connection with the provision of a publicly available electronic communications service.

- The E-Governence Act: imposes on the administrative bodies to use information systems compliant with ther requirements for information security in accordance with the CA.
- eIDAS (Regulation (EU) No 910/2014): defines 'security breach' as an event 'where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme'.
- The Law on Payment Services and Payment Systems (LPSPS) implementing the Payment services (PSD 2) (Directive (EU) 2015/2366) addresses the management of operational and security risks. The Ordinance issued under the LPSPS on No. 3 of the Bulgarian National Bank of 18.04.2018 on the Terms and Procedure for the Opening of Payments

Accounts, Execution of Payment Transactions and Use of Payment Instruments defines ‘operational and security risk’ as a single event or a series of related events not planned by the payment service provider that have, or are likely to have, an adverse effect on the integrity, accessibility, confidentiality, authenticity and / or continuity of the provision of the payment service.

19. **Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?**

(i) Notifications under the GDPR

The GDPR requires data controllers to notify the data protection authority about a personal data breach without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to data subjects' rights and freedoms. It also requires processors to notify controllers without undue delay after becoming aware of a personal data breach. (Article 33 GDPR).

Under Article 34 GDPR, if the data breach is likely to result in a high risk to data subjects' rights and freedoms, then the data controller must also inform them (without undue delay).

According to Recital 85 GDPR, to assess the risk posed to data subjects' rights and freedoms, an assessment should be made of the potential negative consequences. Although this list is not

exhaustive, the GDPR specifies that the potential adverse consequences of a data breach can include material and non-material damage, such as:

- Loss of control over personal data
- Discrimination
- Identify theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality.

(ii) Notifications under the CA

The notification under the CA in the event of the specified incidents occurring should be made by the addressees of the CA (see Question 18) to the respective Sectoral Computer Security Incident Response Team (CSIRT) within two hours of identifying the incident and the complete data should be sent within 5 days (Articles 21, para. 4, 5 and 6; 22, 23 CA).

Notifications have to be submitted following the sample form approved in accordance with an ordinance on the minimum scope of network and information security measures, along with other recommended measures to be adopted by the Council of Ministers under Article 3, para. 2 CA. By-law legislation is yet to be adopted.

The CA provides for the possibility also for persons who are not addresees of the CA to conduct notifications to the CSIRT about incidents that affect the integrity of the provided services by them (Article 27 CA).

(iii) Notifications under the E-Communications Act

(a) Under Article 243b E-Communications Act, the undertakings providing public electronic communications networks and/or services shall immediately notify the CRC on each breach of 'security or integrity, which has significant impacted on the functioning of the networks or services'. The CRC may inform the public or require the undertakings to do that, if it decides that it is in public interest the breach to be announced. The notification procedure is being determined in Appendix No. 4 to General requirements of the Communications Regulations Commission (CRC) in the implementation of public electronic communications. Addressees must provide by using an official form an initial notification to the CRC immediatelty after gaining knowledge of the breach and a final notification after endng of the breach.
(b) Under Article 261c E-Communications Act, in the case of a personal data breach, the undertaking that provides publicly available electronic communications services has to notify the CPDP within three days after the breach has been detected. When the breach is likely to adversely affect the personal data or privacy of a subscriber of publicly available electronic communications services or individual, the undertaking has also

to notify the subscriber or individual of the breach.

Notifications are not required if the undertaking has demonstrated to the satisfaction of the CPDP that it has implemented appropriate technological protection measures to protect the personal data concerned by the security breach. Such technological protection measures are present, if they can render the data unintelligible to any person who is not authorized to access it. If the undertaking has not already notified the subscriber or individual of the personal data breach, the CPDP, having considered the likely adverse effects of the breach, may require it to do so. The notification to the subscriber or individual has to at least describe the following:

- the nature of the personal data breach;
- the contact points where more information can be obtained;
- the recommended measures to mitigate the possible adverse effects of the personal data breach.

In the notification of the personal data breach to the CPDP, the undertaking that provides publicly available electronic communications services has to include in addition to the information under Para. (5) also:

- description of the consequences of the personal data breach
- the measures proposed or taken by the undertaking to address, the personal data breach.

The CPDP has issued in accordance with Article 261d E-COMMUNICATIONS ACT an Instruction No. 1 of 21.12.2016.

concerning the circumstances in which undertakings that provide publicly available electronic communications services are required to notify personal data breaches to customers, the format of such notification and the manner in which the notification is to be made which provides further specifications with respect to the topic.

(iv) Notifications under the eIDAS

Under Article 19, para. 2 eIDAS Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of the CRC of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

(v) Notifications under the LPSPS

A payment service provider licensed by the BNB shall immediately notify the BNB in the case of a major operational or security incident. Where the incident has or may have an

impact on the financial interests of payment service users, the payment service provider shall immediately inform the payment service users of the incident and of all measures he takes to limit the adverse effects of the incident. A payment service provider licensed by the BNB shall provide to the BNB statistical data on fraud relating to payments (Article 99 LPSPS). The payment service provider licensed by the BNB must provide notification to BNB immediately about a major operational or security incident. The payment service provider licensed by the BNB must provide an initial, interim and final notification in accordance with the forms in the Guidelines on incident reporting under PSD2 (EBA-GL-2017-10).

- **Do the laws in your jurisdiction provide individual rights, such as the right to access and the right to deletion? If so, please provide a general description on what are the rights, how are they communicated, what exceptions exist and any other relevant details.**

  As provided by the GDPR, individuals enjoy all of the following rights:

  - To have the information regarding the processing provided to them in a transparent and intelligible manner (Article 12 GDPR)
  - To be informed on the processing of their personal data (Articles 13 and 14 GDPR)
  - To access their data (Article 15 GDPR)
  - To have their data rectified (Article 16 GDPR)
  - To have their data erased (Article 17 GDPR)
  - To processing of their data restricted (Article 18 GDPR)
  - To data portability (Article 20 GDPR)

- To object to the processing of their data (Article 21 GDPR)
- To not be subject to a decision based solely on automated processing (Article 22 GDPR)
- To be informed, in certain instances, of a data breach (Article 34 GDPR).

The controller may refuse, wholly or partially, the exercise of the individual rights, and may not fulfill the obligation to inform individuals on data breaches where the exercise of the rights or the fulfillment of the obligation would create a risk for:

- the national security
- the defense
- the public order and security
- the prevention, investigation, detection or prosecution of criminal offenses or the enforcement of sanctions, including the prevention of threats to public order and security
- other important objectives of broad public interest and, in particular, an important economic or financial interest, including monetary, budgetary and fiscal matters, public health and social security
- the protection of the independence of the judiciary and judicial proceedings
- the prevention, investigation, detection and prosecution of breaches of ethical codes in regulated professions
- the protection of the data subject or the rights and freedoms of others
- the enforcement of civil claims (Article 37a, para. 1 PDPA).

However, for applying any of the above exceptions under Art. 37a PDPA the rules and conditions for their application should be set out in law. These exceptions follow the restrictions permitted by Art. 23 GDPR. Currently, the Bulgarian legislation in this context is not yet developed, which means that in practice the application of the enlisted exceptions/ restrictions

would be rather limited as there are no the necessary rules and safeguards as required by Art. 23 GDPR.

Individuals can exercise their rights by means of a written request to the controller or by another method specified by the latter (Article 37b, para. 1 PDPA). The request may also be filed electronically under the terms of the Electronic Document and Electronic Certification Services Act, the E-Governance Act and the E-Identification Act (Article 37b, para. 2 PDPA). The request may also be filed through actions in the user interface of the information system used for the processing of data, once the individual has been identified with the respective identification means corresponding to the information system (Article 37b, para. 3 PDPA).

The request shall contain the following requisites:

- name, address, national personal identification number or personal identification number of a foreigner or other similar identifier, or other identification data of the individual determined by the controller
- description of the request
- preferred form for obtaining the information when exercising the rights under Article 15-22 GDPR
- signature, date of filing of the request and address for correspondence.

The request may be submitted by a third authorized person, in which case the power of attorney shall be provided together with the request. (Article 37c PDPA)

- **Are individual rights exercisable through the judicial system or enforced by a regulator or both? When exercisable through the judicial system, does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances? Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury of feelings sufficient?**

  As settled with GDPR (Article 79 GDPR), in Bulgaria individual rights are both exercisable through the judicial system and enforced by the national data protection authority – the CPDP.

  Proceedings before the CPDP in relation to the exercise of individual rights are initiated with a complaint filed by the interested party. The CPDP carries out checks, requires documents and has the corrective power to order the controller or the processor to comply with the data subject’s requests for exercise of rights under the GDPR. The order of the CPDP is an administrative measure within the meaning of the Bulgarian Administrative Violations and Penalties Act and may be appealed under the Administrative Procedure Code within 14 days of its receipt. Altarnatively, the PDPC may issue a decision sanctioning the respective behavior of the data controlle or processor and imposing a monetary sanction.

  When individual rights are exercised through the judicial system, the general conditions for claims and damages apply.

Data subjects may claim damages for the damage suffered as a result of the unauthorised processing of personal data by the controller or the processor.

- **How are the laws governing privacy and data protection enforced? What is the range of fines and penalties for violation of these laws? Can PII owners appeal to the courts against orders of the regulators?**

  The GDPR allows for the data protection authority in Bulgaria – the CPDP, to impose administrative fines for violations of the GDPR, dependent on which provisions of the GDPR have been breached, up to:

  - For infringements of any of the obligations of the controller/processor (stipulated in Article 8, 11, 25-39, 42 and 43 of the GDPR) – administrative fines up to 10 000 000 EUR, or up to 20 % of the total worldwide annual turnover of the preceding year of an undertaking.
  - For infringements of the principles of processing inherent in the Regulation, the data subjects' rights, the transfers of personal data to a recipient in a third country, any obligations pursuant to Member State law and pertinent to special processing situations, as well as non-compliance with an order or a temporary definitive limitation by the supervisory authority - administrative fines up to 20 000 000 EUR, or up to 4 % of the total worldwide annual turnover of the preceding financial year of an undertaking.

  For violations of some specific rules of the PDPA (falling with the permittd derogations under GDPR), the PDPA refers to the sanctions under GDPR.

- **Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.**

In addition to the general GDPR provisions, special rules with regard to the processing of personal data in Bulgaria are settled for the following matters:

- General prohibition on making copies of ID cards, driver's licenses, or residence permits unless explicitly required by law (Article 25d PDPA)
- General prohibition on public access to information containing data subjects' national personal identification number unless explicitly required by law (Article 25g PDPA; cf. Question 16 above)
- Obligation for employers in their capacity of data controllers, to adopt special rules and procedures when implementing or introducing within their organisation:
  - whistleblowing systems
  - restrictions on the use of in-house resources, and
  - systems for access control, working time and work discipline.
  (Article 25i PDPA; Cf. Question 8 above)
- Retention period of data collected for the purposes of personnel recruitment may not exceed 6 months unless the applicant has consented to a longer period (Article 25k, PDPA; Cf. Question 5 above)
- Obligation for the controller to obtain consent from a parent or guardian exercising parental rights for the processing the personal data of a minor under the age of 14 based on consent (Article 25c PDPA; Cf. Question 5 above)
- When processing deceased persons' data, obligation for the controller to:
  - have a legal basis
  - implement appropriate measures so that the processing does not adversely affect the rights or freedoms of others or any public interest, and
  - provide access to and a copy of the processed personal data to the successors of the deceased persons and other persons with legal interest.
  (Article 25f PDPA)
- When processing personal data for the purposes of journalistic, academic, artistic and or literary expression, the controller must balance freedom of expression, right to information, and privacy in compliance with the criteria set out in the PDPA,

including:
- the nature of the personal data
- the impact which the disclosure of the personal data or its public announcement would have on the integrity of the data subject's personal life and good reputation
- the circumstances under which the personal data has become known to the data controller
- the character and nature of the statement through which the rights to freedom of expression and to information are being exercised
- the relevance of the disclosure of personal data or its public announcement for the purposes of clarifying an issue of public interest
- the data subject's role in society, such as whether the person has a high state post such as president, vice president, parliament member, or if a person has lower protection of personal integrity or whose actions have impact on society because of the person's activity or role in the public life
- the data subject's role in disclosure, such as whether the data subject has actively contributed to disclosing its personal data or information about its personal or family life
- the purpose, content, form, and consequences of the resulting statement
- the correspondence of the statement with the citizens' fundamental rights, and
- the other relevant circumstances. (Article 25h PDPA)

- **Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies – how are these terms defined and what restrictions are imposed, if any?**

(i) Profiling

As regards profiling, GDPR applies. No additiona national legislation has been adopted.

According to Article 22 GDPR the data subject has the right not to be subject to a decision based solely on automated

processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Such processing is only allowed if the decision is

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

(ii) Monitoring

As regards ‘employer whistleblowing systems, restrictions on the use of in-house resources, and access controls’ as well as ‘large-scale processing of personal data or systematic large-scale surveillance of publicly accessible areas’, please refer to Question 4.

(iii) Cookies

Bulgarian local requirements on cookies consent follow the provisions of the Cookie-Directive (Directive 2002/58/EC amended by Directive 2009/136/EC). Bulgaria has implemented the Cookie-Directive in the Electronic Commerce Act (EA). In conjunction to the E-Commerce rule, GDPR provisions are also applicable as far as the use of cookies may constitute processing of personal data.

Pursuant to Article 4a EA the provider of information society

services may store information or receive access to information stored in the terminal device of the service recipient (i.e. the user), provided that: 1. the user is provided with clear and exhaustive information in accordance with Article 13 GDPR; and 2. the user is provided with the option to refuse the storage or access to information, meaning to refuse cookies prior to their use by the service provider. The wording of Article 4a slightly differs from the original wording of the Cookies Directive, but introduces an opt-in regime for the use of cookies, meaning that prior user's consent is required for the lawful use of cookies.

Under Bulgarian law, there are no specific requirements regarding the definition or the form of the 'consent' and the consent for the use of cookies should be interpreted by reference to the definition in the GDPR. Consent is not required only for cookies that are necessary for: 1. transmission of communications over the electronic communication network; or 2. provision of an information society service explicitly requested by the user. Thus, for the use of non-essential cookies (e.g., marketing and analytics cookies, etc), a prior consent must be obtained.

- **Please describe any laws addressing email communication or direct marketing?**

  In addition to the general rules established with the GDPR,

Bulgarian legislation establishes a general opt-in regime for sending unsolicited commercial communications to natural persons and a general opt-out regime for sending such communications to legal persons, and consists of the following laws:

- The E-Commerce Act: Contains provisions related to the regime of unsolicited commercial communications, namely:
  - Unscolicited commercial communications cannot be sent to natural persons without their prior consent (Article 6, para. 4 E-Commerce Act).
  - Unscolicited commercial communications have to be clearly distinguishable as such at the very moment of their receipt by the recipient (Article 6, para. 1 E-Commerce Act).
- The E-Communications Act: Contains provisions related to the regime of direct marketing communications, namely:
  - Sending direct marketing and advertising communication is allowed solely in case prior consent has been obtained (Article 261, para. 1 E-Communications Act).
  - In case electronic contact details have been obtained in the context of a provision of goods or services, these contact details may be used for sending marketing and advertising communications for similar goods or services (Article 261, para. 2 E-Communications Act).
  - The communication must allow for a clear identification of the sender and shall contain a valid email address where a request for unsubscription could be sent (Article 261, para. 5 E-Communications Act).
- The Consumer Protection Act: Contains provisions related to the regime of unsolicited business communications, namely:
  - Sending unsolicited commercial communication to consumers is prohibited unless they have provided their prior consent.