THE NEW EU DATA PROTECTION REGIME IN BULGARIAN LAW AND PRACTICE[1]

The new EU data protection package entered into force in May 2018, following a protracted legislative process. The package comprised a General Data Protection Regulation (Regulation 2016/679, GDPR) and a lesser-known Law Enforcement Directive (Directive 2016/680, LED). The GDPR, in particular, seeks to "Europeanise" data protection law and to render it more effective: by introducing a regulation rather than a directive, an attempt is made to minimise national divergence while significant new avenues for private redress and public enforcement are introduced. Although the responsibility for public enforcement of the framework lies primarily with national supervisory authorities (NSAs), the creation of a new European body with the power to issue authoritative opinions and, in specific cases, binding decisions has a centralising effect on data protection enforcement. The hope is that the changes brought about by the GDPR will ultimately enhance the effectiveness of the EU Charter rights to data protection and privacy. Yet, despite this shift towards a truly European legal framework for data protection, and unusually for a regulation, the GPDR leaves much responsibility to the national legislature, NSAs and courts.

This new regulatory framework raises substantive, procedural and institutional issues. Those with an interest in procedural and institutional matters will note that the GDPR sets out detailed provisions on remedies, liability and penalties. These provisions specify high administrative fines and provide for the possibility of criminal sanctions, as well as introducing provisions providing for representative actions by non-profit organisations. These detailed remedies, avenues for redress and sanctions will need to be accommodated within the national legal system in a way that is compatible with the general principle of national procedural autonomy. From a substantive perspective, the application of the EU Charter rights to data protection and privacy has had a transformative effect on the fundamental rights landscape in Europe. How the EU Charter has impacted upon domestic legal systems in this area as well as the impact of the GDPR on other rights, such as freedom of expression, which is the most touchy matter.

Furthermore, the CJEU has been pushing the boundaries of the Charter right to respect for privacy in the context of law enforcement. The relevance of this jurisprudence to domestic national security interests, and thus issues of sovereignty, remains contested.

Similarly, whether individuals should have a right to delete their data from the de facto public record (for instance, a search engine service like Google) when there is a countervailing public interest in this information is hotly contested.

Related to that and further more issues the present text answers based on Bulgarian legislation a few questions structured around four key areas of inquiry: A. Setting the Scene; B. The Reception of Substantive GDPR Provisions in the National Legal Order; C. Domestic Enforcement of Data Protection Law; D. Data Processing for National Security Purposes.

The rave around the GDPR before May 2018 made data processing a very popular and modern topic for discussions, seminars, books, businesses. The hysteria for "GDPR compliance with" did not spare Bulgaria. In fact, our country has had a Personal Data Protection Act (PDPA) since 2002, even before Bulgaria joined the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (The Convention No 108).

[1] This text contains preliminary answers to the questions posed in The Hague 2020 FIDE Congressional Questionnaire; FIDE is a *Federation International de Droit Europeen (*https://www.fide-europe.org/*);* The Congress in 2022 will take place in Sofia.

The Main National Legal Instruments That Have Been Introduced To Implement The GDPR

Bulgarian Personal Data Protection Act[2] (PDPA) does not deviate from the European Commission guidance on direct application of GDPR and its reconciliation with the issues which GDPR leaves to the discretion of and legal solution offered by each Member State. Following that the national legislator adapts the existing Law to the new requirement of GDPR. First of all, the redundant provisions as well as those which were not in compliance with GDPR have been removed.

The national legislator accepts the progressive approach to complying with EU data protection legislation by including the GDPR concept and the rules of Directive (EC) 2016/280 in one common legal act. Even the difference between the legal nature of both EU law acts, Regulation and Directive, such approach is logical and successful in principle, as well as referring to legislative technique philosophy. To gather in one single legal act the common data protection rules and to underline the specific requirements because of the nature of the processes referred to in Directive (EC) 2016/680 seems as codifying the national legal framework in the field of protection of individuals with regard to data processing.

The first group of national legal instruments concerns the issues where GDPR gives the opportunity to or requires a Member state to create its national solutions. Such spheres are:

(i) Rules on processing of national identification number: Actually, the personal identification number which was created as a really unique mark to identify any person and includes in itself information about date of birth, area of origin and gender, is one of the least secret personal data in our daily life. Especially if one is an active person who is a partner in a company, possesses real estates, etc. So much so that in 2018, a discussion about the personal identification number not to be the only means of identifying the user started. Nowadays, PDPA permits information containing personal identification number to be available only if a special law explicitly requires it public access to. Otherwise, the controllers providing services by electronic means are required to take appropriate technical and organisational measures to ensure that the personal identification number is not the only means of identifying the user (in this sense: art. 25g paragraph 2 of PDPA);

(ii) Data processing for journalistic purposes and for the purposes of academic, artistic or literary expression: the PDPA requires the freedom of expression and the right to information to respect the data subject privacy. In order to boost finding of "the golden mean" the national legislator has put several criteria on the basis of which the evaluation if the relevant data processing has a real value for the society should be done, e.g. is it of public interest or it is just a piece of information which is interesting for the members of the public, i.e. it has the characteristics of gossip.

(iii) Certain aspects of data processing by employers/appointing authorities: the legal instruments applied in this area intend to reach the balance between the legitimate interest of employers or appointing authorities and the fundamental rights and freedom of employees. The principle adopted by the legislator is that employees should be informed about each of the measures/systems/organization which is applied by the employer or appointing authority in favor of their legitimate interest which should not exceed the nature of the activity, special needs and available resources of the enterprises. There are special rules concerning collecting, storing and returning and/or erasing or destroying the originals or notary certified copies of any documents candidates are requested to submit in staff selection procedures.The storage period is limited to six months unless the applicant has given consent for a longer period of storage. When the period of time expires, the employer or appointing authority shall erase or destroy the documents containing personal data unless otherwise provided for by a special law.

[2] PDPA in English: https://www.cpdp.bg/en/index.php?p=element&aid=1194

(iv) Despite the GDPR principle being inapplicable to the deceased persons' data, the national legislator has provided for rules regarding the processing of personal data of deceased persons. PDPA requires a legal basis for the deceased persons' data processing and the controllers or processors are obliged to take the appropriate measures so that the rights and freedoms of others or a public interest should not be adversely affected. The persons authorized to get access to personal data of a deceased person, including by providing a copy, are the heirs of the person or other persons with a legitimate interest.

(v) Data processing for National Archiving Fund purposes is found as processing in public interest and Articles 15, 16, 18, 19, 20 and 21 of GDPR and shall not apply in such cases (that exception is under Article 25k of PDPA). In the case where personal data is processed for statistical purposes, Articles 15, 16, 18 and 21 GDPR shall not apply (Article 25l PDPA).

(vi) The national legislator finds data processing for humanitarian purposes as lawful in case it is operated by public bodies or humanitarian organisations, as well as when processing concerns cases of disaster within the meaning of the Disaster Protection Act. In the case of such processing purposes Articles 12 to 21 and Article 34 of GDPR are not applicable.

(vii) Obligations in large-scale processing are seen in Article 25e of PDPA: The data controller or processor shall adopt and apply rules for large scale personal data processing or for a large scale systematic monitoring of publicly accessible areas, including video surveillance, if the controller or processor implements appropriate technical and organisational measures for safeguarding the rights and freedoms of data subjects. The rules on large scale systematic monitoring of publicly accessible areas shall state the legal grounds for setting up a monitoring system, its scope and means, storage period of the information records and their erasure, the individuals' right of access, the provision of information to the public about the monitoring, as well as restrictions with regard to the access of third parties. In paragraph 2 of the same article, the national legislator obliges the NSA to issue guidelines to data controllers and processors for the performance of the obligations detailed above and make them available on NSA Internet site. PDPA says that *"Large-scale (processing operations) shall be monitoring and/or processing of personal data of a significant or unlimited number of data subjects or amount of personal data, where the core activities of the controller or the processor, including the means by which these activities are carried out, consist of such operations".*

The second group of specific national legal solutions concerns the restrictions permitted under article 23 of GDPR: the way and the terms to execute the rights under article 15 – 22 of GDPR.

The third group of legal instruments concerns the transition of Directive (EC) 2016/680. There are certain differences in the principles adopted by the Directive. For example, the principle of transparency is not the leading one in the case of data processing for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties. The storage period regarding those data differs also from the period for storage of personal data in the case of regular processing.

The Bulgarian Law And Jurisprudence's Interpretation of EU Charter Right to Data Protection

Actually, even now EU Charter is a certain exotic instrument in comparison with ECHR. As far as the Convention is an international legal instrument it is easy to find the spot of its application. But the EU Charter supposes to have its limited application (within the framework of EU Law scope) so our national legislator does not make very deep differentiation between the "respect for private and family right" (art. 7 of EU Charter) and "personal data protection" (art. 8) as far as the understanding of the national law is that the institute of "personal data" includes the privacy of the personal and family relationships.

So, our national legislation and practice accept and rely on the common, GDPR's, principles and rules for personal data protection and our national law on PDP does not include any special provision to respect private and family right. On the other hand, private and family life privacy is stated to be one of the criteria in search for the balance between the freedom of expression and the right to information and the right of personal data protection in article 25h of Personal Data Protection Act. In article 25h, paragraph 2item 2, the national legislator requires that "the impact that the disclosure of the personal data or the publishing of the data would have on the data subject's privacy and reputation" to be evaluated searching for the balance aforementioned.

The Principles of 'Fair' Processing; Purpose Limitation and 'Data Minimisation' in Bulgarian Law and Jurisprudence

The national jurisprudence and the practice of the Commission for Personal Data Protection (Bulgarian NSA) usually interpret those principles in the most common way, as it is required by the EU law and CEC jurisprudence. The understanding of the NSA and the courts for an eventual difference or nuance in the interpretation, could by noticed when the requirements of the basic principles of PDPA should be applied together with the requirements of other special laws as Anti-money Laundering Measures Act, etc. when even the purpose of data processing is different, the controller has the obligation to collect more data because it fulfills its obligation under that law. Other examples are Occupational Health Authorities, who maintain health records by virtue of their own regulations and not because they have been assigned to do so by the administrator. The NSA follows the same philosophy in its Opinion on the Draft of the Protection and Development of Culture Act where the NSA finds that collecting data of young people beneficiaries of E-cards for cultural activities is a fair processing: after the law adoption such collection will be based on the controller's (Ministry of Culture) legitimate interest or its legal obligation (it depends on the point of view).[3]

The constant practice of our Commission for Personal Data Protection calls for a minimalist approach to the use of personal data, especially the data of those individuals who are not public persons and have no direct relation on a debate of public interest. The exception to allowing deviations from such an approach is when that approach would impede the exercise of the right to information.[4]

The Omnipresent "Consent", "Legitimate Interest" and The Digital Environment

Obviously, the controllers find the "consent" of the data subject as one of the most easily obtainable reasons for data processing. Many of them put themselves in the stalemate of not obtaining the consent requested (by the subject) and thus unable to process the data lawfully, although there are other grounds for processing for the same purpose for which they requested consent. In order to avoid that Catch 22 the NSA has published Guidelines where the situations when consent should not be required are pointed out and explained in detail.[5] Those Guidelines were published after 25th of May 2018 and up to that moment quite few controllers had already got in the position waiting for data subject consent … which will probably never come.

So, from a formal point of view, any further processing of data for the purpose for which consent was previously sought should be considered illegal, even if another ground for processing the data for the same purpose exists. The same "dead end" situation is encountered when the controller had started

[3] That NSA Decision (unfortunately, all NSA documents are only in Bulgarian) is published on: https://www.cpdp.bg/index.php?p=element_view&aid=2085

[4] NSA Decision: https://www.cpdp.bg/index.php?p=element_view&aid=2186

[5] The Guidelines: https://www.cpdp.bg/?p=element_view&aid=2117

to process the data on the consent of the data subject although other grounds had existed and then later, the data subject decided to withdraw its consent.

It is evident that "the consent" is the most uncertain ground for data processing: the lawfulness of controllers' activities depends on the data subject's position/mood/emotions. However, the case is not this when data processing is based on the controller's "legitimate interest".

There is no legal definition of "legitimate interest" but the courts give the following definition: in order to be recognized as "legitimate" the source and the purpose of the interest should be to satisfy a particular human need, to be admissible by the law, i.e. legal remedies are provided for its enforcement/satisfaction (subjective rights), and in case such rights are not expressively provided for, they are admissible in the light of the general principles of law. Obviously there are cases where the legitimate interest is expressly defined by the law and the controller should not hesitate to proceed with data. But if legitimate interest does not exist by law but because of the concrete situation, then an additional evaluation is required. The court is competent to make such an evaluation. The main criteria should be whether the data processing would be in favor of revealing the objective truth, respectively to the benefit of either of the parties. A simple example of that is when at the time of court proceedings one of the parties would like to present before the court information about the counterparty, which means "personal data" and for its dissemination any consent is required. Surely, the counterparty will not give her/his consent. So, the deciding court should assess whether that information has its "added value" for the party within the frame of the process. Then the court could permit or deny the information to be obtained by the party concerned. Specifically, in Bulgarian law, the order of receiving it officially, i.e. legally, is in Art. 186 of the Code of Civil Procedure, which provides for the possibility, after a positive assessment of admissibility and relevance, that the determining court issue a court certificate whereby the institution having the requested data cooperates and provides them. It should be underlined in this context that it is not enough for the controller to have the information she/he wishes to present before the court or any third party at her/his disposal, but she/he needs a legal ground to disseminate that info.[6]

Personal Data as "Counter Performance" for Contract Signing

"Counter performance" is easily visible during the process of labor contract signing. Usually, employers require a lot more personal data than they really need to hire the candidate and to prepare and sign the labor contract. An example of such unreasonable requirements whose fulfillment is a condition *sine qua non* for the employment relationship to be established are the following requirements of the employers: (i) number of personal identification card or passport although the law (Labor Code and Ordinance No 4/May 1993 for the documents necessary to sign a labor contract) requires only personal identification number; and/or (ii) "criminal record certificate" although there is not any special law which requires such info for the position the candidate applies for; and/or (iii) the employers keep the job history book of the employees in the company's/enterprise's archive office: the job history book ,being a private document of each person where all his/her jobs salaries, eventual penalties and praises are enlisted, and as such its storage should be with the holder. Neither the law nor the Ordinance require its storage with the employer but it is a "common practice" to leave it with the employer at signing the employment contract; and if the employee refuses the employment contract could be denied by the employer, at least that was the situation before 25 May 2018.

[6] The Decision on that case is Resolution No 10776 from 10.07.2019 on administrative case No 595/2018 at the inventory of Supreme Administrative Court (http://www.sac.government.bg/court22.nsf/d6397429a99ee2afc225661e00383a86/1a08ddde3fd74702c22584310049a706?OpenDocument)

In most of the cases such unfounded document requests are placed by the employers unwillingly, due to low levels of GDPR awareness.

Automated Decision-Making – Yes or No

In article 52 paragraph 1 of national PDPA the Bulgarian legislator has accepted a wording of the presumptive ban of article 22 paragraph 1 from the GDPR which allows the data subject to be subject to a decision based solely on automated processing, including profiling, if such does not produce *adverse* legal effects concerning him or her. Admitting this wording, the refinement "*unless this is provided for in Union law or in the legislation of the Republic of Bulgaria"* sounds like even if potential "adverse effects" could occur, automatic data processing and profiling is acceptable if either law allows it. Surely, the characteristic "adverse" could be interpreted quite widely and in a bias way.

In paragraph 2 of article 52 of PDPA, the national legislator has permitted an automated processing even on the special categories of personal data (article 9 from GDPR) as long as suitable measures to safeguard the rights and freedoms and legitimate interests of the data subject are in place.

In any case, an impact assessment is required as the minimum elements of the assessment process are listed in article 64 paragraph 2 of PDPA: (i) a general description of the envisaged processing operations; (ii) an assessment of the risks to the rights and freedoms of data subjects; (iii) the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Chapter taking into account the rights and legitimate interests of data subjects and other persons concerned. Discrimination impact is prohibited in any case (look Article 52 paragraph 4 of PDPA).

The controller and the processor are required to keep logs for at least the following processing operations: collection, alteration, consultation, disclosure including transfers, combination and erasure, so that those logs could be used to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. The logs shall be used solely for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. The time limits for storage and archiving of the logs should be established by the controller or processor (Article 64 of PDPA).

There are certain stages of automated data processing where strict control is required by the law to be applied by controller and/or processor as a measure to protect the rights and freedoms of natural persons. Those areas are: **(i)** equipment and data access (no unauthorised person access to processing equipment used for processing of personal data and/or to data not covered by the personal access authorisation); (ii) data media control (authorised reading, copying, modification or removal of data media only); (iii) storage control (prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data); (iv) users control (authorised persons using data communication equipment only); (v)communication control (ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment); (vi) input control (ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input); (vii) transmit control (prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media).

The national legislator provides that the rules of processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties, safeguarding against and prevention of threats to public order and security (Charter VIII of PDPA) must be applied in case of thoroughly or partly automatic processing and profiling (Article 43

of PDPA). One might say that such legislative approach to a certain degree remedies the deviation of article 22 GDPR conception.

The Right to Erasure at National Level

Actually, the right to erase is a source of disputes almost only within the context of journalist's activities where it is a great challenge to find the balance between right to privacy of the personal life, freedom of expression and right to information. Unfortunately, in this case the "balance" is not a physical category and it is not concentrated in one single cross-point. Actually, it is the interest of the individuals not their rights that are the leading criterion; and sometimes it is the one who is stronger who wins, not the rightful one. Detailed considerations are given below, in item 8.

The right of erasure is an obligation for the controller under the hypothesis of 25a PDPA where the data controller or the processor have been provided by with personal data without legal basis pursuant to Article 6 (1) of Regulation (EU) 2016/679 or contrary to the principles under Article 5 of the same Regulation, they shall return such data within a period of one month after having become aware of it or, if this is impossible or would involve disproportionate efforts, shall erase or destroy the data. The erasure and destruction shall be documented.

In case of incorrect data even if the processing is for the purposes of for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public order and security, the data should be rectified or erased by the controller or by the recipient in cases of data transmission.

In case the law says nothing, the controller is competent to determine the data storage period. In case the controller decides the storage period to be extended, a special written and motivated decision should be issued.

Even though the understanding that "the right to erase" is not an absolute right, there are enough strong sanctions in case the controller denies unreasonably to erase the data. The data controller shall maintain a record of the categories of personal data processing activities which shall contain where possible, the envisaged time limits for erasure of the different categories of data.

The cases where the controller is obliged to erase the data are provided in article 56 paragraph 2 of PDPA: (i) where the data collected by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public order and security are processing other than the purpose for which that data have been originally collected; (ii) where the processing is not necessary for the exercise of powers by a competent authority for the purposes referred to in previous sentence and where such processing is not provided for in Union law or in a statutory instrument which defines the purposes of the processing and the categories of personal data which are processed; (iii) where the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation without that being strictly necessary, if there are appropriate safeguards for the rights and freedoms of the data subject, and it is provided for in Union law or in the legislation of the Republic of Bulgaria (Article 51 PDPA).

The controller is authorised to deny erasure of the data where this is necessary in order to (i) avoid obstructing official or legal checks, investigations or procedures; (ii) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (iii)

protect public order and security; (iv) protect national security; (v) protect the rights and freedoms of others.

The "right to erase" is almost absolute in the relations between the data controller and the data processor as the last one is obliged to erase the data if the controller requires that without the option to refuse unless the conditions and procedure for the processing are provided for in Union law or in the legislation of the Republic of Bulgaria.

The right to erase could be executed by the NSA, respectively the Inspectorate, in exercising supervision, the supervising authorities have power to order the controller or processor to bring data processing operations into compliance with the applicable provisions, including to order the rectification, completion or erasure of personal data or restriction of the processing.

Right to Data Rrotection v. Freedom of Expression

This is one of the most controversial matters when it comes to personal data processing. Both law and the practice are used to talk about the balance between the freedom of expression and the right to information on the one hand and, the privacy of personal and family life on the other hand, as main criteria to find data processing lawful; however, everyone is quiet when it comes to the characteristics of that mythical balance.

When it comes to Bulgarian legislation concerning data processing for journalistic purposes and for the purposes of academic, artistic or literary expression, GDPR does not influence much the main principle adopted by the Bulgarian legislator in 2002, when the PDPA was first drafted. What is novel here, is that the amendment introduces criteria on the basis of which it should be assessed if the above mentioned balance exists or not.

The criteria under article 25h paragraph 2 of PDPA are as follows:
(i) Nature of the personal data;
(ii) The impact that the disclosure of the personal data or the publishing of the data would have on the data subject's privacy and reputation;
(iii) The circumstances under which the personal data became known to the controller;
(iv) The character and nature of the statement under which the rights of freedom of expression are exercised;
(v) The significance of the disclosure of personal data or the publishing of the data for the clarification of a matter of public interest;
(vi) Taking into consideration whether the data subject occupies a position under Article 6 of the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act or is a person who, because of his activity and public status enjoys lesser protection of his privacy, or whose actions impact the society;
(vii) Taking into consideration whether the data subject has contributed with his actions for the disclosure of his personal data and/or of information about his private and family life;
(viii) The purpose, content, form and consequence of the statement when the rights pursuant paragraph (1) are exercised;
(ix) The compliance of the statement for exercising the rights of freedom of the expression and the right of information with the fundamental rights of citizens;
(x) Other circumstances relevant to the case.

At the moment of drafting this text there is not any court jurisprudence on these criteria application and/or evaluation. There is not any opinion of NSA either. But there is a Request signed by fifty members of the Parliament asking The Constitutional Court to find those criteria in contradiction of national Constitution and ECHR. BAEL has been invited to present an opinion on this request and the position declared by our Association was one in defense of the criteria. The mainline of our position is that the information journalists make available should be really of great importance for society,

for its judgments and knowledge and not just a piece of information that is interesting for the people, e.g. do not disseminate any information only because it makes the circulation of the newspaper high. There are a lot of examples in our reality of unnecessary private details made available to the public despite those details being irrelevant to the activity and/or position of the public person the society should be informed about.

One of the latest principal NSA opinions on these matters concerns data processing by the Prosecutor's Office of the Republic of Bulgaria when publishing press releases and providing information for journalistic purposes. The position of NSA is the following:

> *"The publication of personal data of accused persons in pre-trial proceedings on the websites of the prosecutor's offices, as well as their provision to the media for journalistic purposes, is lawful when there is a legal obligation or there is an overriding public interest". In cases where for the public purpose it is impossible or inappropriate to publish the information in an anonymous or pseudonymized form, then the indication of the name, position or place of work of the accused would be sufficient to achieve public awareness, and the publication of a personal identification number and any relations with third parties who are out of the process, etc. would be excessive. As a general rule, the personal data of other participants in pre-trial proceedings, such as witnesses, experts or related to these categories of third parties, etc., should not be published or otherwise disclosed, as long as there is no legal obligation to do so or overriding public interest. An exception could be made with respect to persons holding high public positions within the meaning of Art. 6 of the Anti-Corruption Law and the Forfeiture of Illegally Acquired Property or another Person, which by its nature has an effect on the public, or where the publication of the information protects the vital interests of the data subject. In all cases of publishing personal data of participants in pre-trial proceedings or providing them to the media, the principles for processing personal data in Art. 5 of Regulation (EU) 2016/679, in particular the principles of minimizing data in order to achieve the objective, accuracy of data and limitation of storage time, should be apllied*."

Though this is one of the most specific and detailed opinions of the NSA referred to data processing to journalistic purposes, it uses general expressions as "overriding public interest" and "effect on the public" which leave the final evaluation in the hands and conscious of the author of the press release.

The national legislator provides for the following exemptions under article 85 paragraph 2 GDPR: articles 6, 9, 10, 30, 34 and Chapter V of Regulation (EU) 2016/679. Another exemption is that of article 25c PDPA. Actually, this provision concerns the rights of data subjects under the age of 14 and requires the administrator to make sure that consent for data processing from the parent with parental rights or by a legal guardian is given. So, by this provision even the privacy of a little child could be less important than the freedom of expression and right of information. This report finds that exemption excessive and unfair. Even though the place of the following comment is misplaced, the national legislative decision that only persons below 14 are to be considered "children" is at least strange having in mind that according to our national law persons up to 14 years old are infants, between 14 and 18 are minors (and their civil rights continue to be exercised with parental consent) and only after 18 do they receive full rights. So, the legal decision not to require parental consent for data processing concerning children of all ages for journalistic purposes is not safe for children and for their future as a whole.

Where data processing is for journalistic purposes and for the purposes of academic, artistic or literary expression, the data controller or processor may deny the data subjects, fully or partially the exercise of the rights pursuant Articles 12 to 21 of Regulation (EU) 2016/679. (Article 25h paragraph 3 point 2 PDPA)

The autonomy of data processing for journalistic purposes and for the purposes of academic, artistic or literary expression, is fully protected with the provision of paragraph 4 of article 25h PDPA: *"the exercise of the powers of NSA pursuant to Article 58 (1) of Regulation (EU) 2016/679 shall not affect the secrecy of information sources"*.

Another group of exemptions are provided for by the national legislator where personal data are processed for the purposes of creating a photographic or audio-visual work by means of capturing the image of a person in the course of the public activity or in a public place: in those cases Article 6, Articles 12 to 21, and Articles 30 to 34 of Regulation (EU) 2016/679 do not apply.

Within Bulgarian national legislation one of the most popular ways to reach officially any information is allowed by the Access to Public Information Act where any citizen of the Republic of Bulgaria, foreigner or individuals with no citizenship are entitled to access to public information subject to the conditions and the procedure set forth in the act, unless another act provides for a special procedure to seek, receive and impart such information, for example if the information required is "classified information", i.e. any information which concerns national security and the like .

Surely, that act does not apply to the access to personal data, as it is written down in article 2 paragraph 5 of the Access to Public Information Act. Actually, such restriction is a bit hypocritical because the information that is often sought and owed under this law is "personal data" and nothing more.

About National Supervisory Authority – Composition, Competence, Relations

The national supervisory authority is the Commission for Personal Data Protection (CPDP). It is created as independent supervisory authority which protects the individuals with regard to processing of their personal data and access to these data, as well as the supervision on the compliance with Regulation (EU) 2016/679 and with national legislation. Surely, CPCP provides assistance with the implementation of the state policy in the personal data protection field.

There is an "alternative" supervising authority provided for in PDPA - the Inspectorate of the Supreme Judicial Council (The Inspectorate) – which exercises supervision and ensures compliance with Regulation (EU) 2016/679, with PDPA and with the statutory instruments in the field of personal data protection upon the processing of personal data by the courts when acting in their judicial capacity and by the prosecution and the investigating authorities when acting in the judicial capacity for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties. Where the courts and the prosecutor's office and the investigation's office act as employer the competent supervising authority is the Commission for Personal Data Protection.

The CPDP consists of a Chairperson and four members who are elected by the National Assembly after a nomination by the Council of Ministers for a five-year term and may be elected for one more term. The Commission adopts decisions by a majority of the total number of its members. The meetings of the Commission are open to the public. The Commission may decide to hold closed meetings. The CPDP report its activity to the National Assembly by 31st March each year.

Eligible to be members of the Commission are Bulgarian citizens who hold a university degree in information science or in law or hold a master's degree in information technology and have not less than ten years working experience. Surely, the candidates should not been sentenced and/or have conflict of interests working another job instead of scientific research or teaching. A qualified lawyer who meets the requirements under Paragraphs (1) and (2) is elected chairperson of the Commission.

The Commission fulfils the tasks pursuant to Article 57 of Regulation (EU) 2016/679. Other duties of the CPDP are to analyse and exercise supervision and to ensure compliance with Regulation (EU) 2016/679, with PDPA and with the statutory instruments in the personal data protection field, except for the cases which concern issues within the framework of Directive (EC) 2016/680 (in which the Inspectorate with Supreme Judicial Council is the competent supervisory authority). The CPDP is competent to issue secondary legislation acts in the personal data protection field, including instructions, guidelines, recommendations and best practices in connection with personal data protection. The CPDP ensures the implementation of the decisions of the European Commission in the personal data protection field and the implementation of the legally binding decisions of the European Data Protection Board under Article 65 of Regulation (EU) 2016/679 also. The CPDP participates in international cooperation with other personal data protection authorities and international organisations on personal data protection issues and in the negotiations and the conclusion of bilateral or multilateral agreements on matters within its competence. The CPDP is competent to organise, coordinates and provides personal data protection training.

Surely, the CPDP is the competent body to exercise the powers pursuant to Article 58 of Regulation (EU) 2016/679.

The Chairperson and the members of the CPDP exercises control by means of prior consultation, inspections and joint operations in compliance with Regulation 2016/679 and with PDPA, especially in cases where data are processed for the performance of a task carried out in public interest, including processing in relation to social protection and public health. In such a case, the CPCD may authorise the processing before the period referred to Article 36 (2) of Regulation (EU) 2016/679 expires. The prior consultation shall take place pursuant Article 36 (2) and (3) of Regulation (EU) 2016/679.

Inspections will be conducted on the initiative of the CPDP, at the request of stakeholders, or after an alert has been submitted. Where there is a need, any expert opinion is allowed.

The CPDP conducts accreditation of certification bodies in pursuant Regulation (EU) 2016/679 on the basis of the requirements laid down by the CPCD or by the European Data Protection Board. The accreditation is issued in accordance with Article 43 (2) of Regulation (EU) 2016/679 for a period of five years and may be renewed. The certification criteria, mechanisms and procedures, seals and marks are laid down in an Ordinance adopted by the CPDP. The Ordinance shall be promulgated in the *State Gazette*. As of September 2019 no such Ordinance has been issued.

The CPDP approves codes of conduct by sector and field of action pursuant to Article 40 of Regulation (EU) 2016/679. Bodies for monitoring the codes of conduct will be authorised by CPDP, with compliance of Article 41 of Regulation (EU) 2016/679.

The CPDP maintains the following public registers: (i) of data controllers and processors which have designated data protection officers; (ii) of accredited certification bodies; (iii) of codes of conduct pursuant Article 40 of Regulation (EU) 2016/679.

The following registers maintained by the CPDP are not public: (i) of the infringements of Regulation (EU) 2016/679 and PDPA, as well as of the measures taken in accordance with the exercise of the powers referred to in Article 58 (2) of Regulation (EU) 2016/679; and the (ii) register of the notifications of personal data breaches under Article 33 of Regulation (EU) 2016/679.

The CPDP is a state budget financed legal person. Its Chairperson is a first level spender which means that the President of the CPDP is authorised to spend the money at its own discretion but within the frames laid down by the law. For example, there are special law provisions on how the monthly

remuneration of the Chairperson and the CPDP members should be formed: the members of the Commission shall receive basic monthly remuneration equivalent to 2.5 average monthly wages received under labour and civil service contract in accordance with the information provided by the National Statistical Institute as the basic monthly remuneration shall be recalculated every three months, taking into consideration the average monthly wage for the previous three months. The Chairperson of the Commission shall receive a monthly remuneration which is 30 per cent higher than the basic monthly remuneration of the members of CPDP. Up to Sept 2019 the officially declared (by National Statistic Institute) average remuneration is BGN 1253 or EUR 637.

All CPDP staff including the Chairperson and the members of the Commission are entitled to presentable clothing with a value of up to two minimum wages each year, and the financial resources shall be allocated from the budget of the CPDP. The individual amount of the financial resources is determinable by the Chairperson under terms and procedures previously established.

The CPDP has its own income, different from the state budget funds. Such are the fees charged for the training organized by the CPDP and certificates issued, the income of the fines imposed by CPDP and upheld by the court, European Union financing programmes and projects, etc.

Complaint-Handling Strategy

In cases of infringement of his/her rights pursuant GDPR and national PDPA, the data subject shall have the right to bring the infringement before NSA (both CPDP or The Inspectorate) within six months after having become aware of the infringement but no later than two years after.

NSA shall inform the complainant of the progress of the complaint or of the result within three months after the infringement has been brought to the attention of it. This way there is not a dead line in which the NSA shall issue its decision. So, it supposes such a term should be reasonable.

The decision issued by NSA may apply the measures referred to in points (a) to (h) and (j) of Article 58 (2) of Regulation (EU) 2016/679 or in Items 3, 4 and 5 of Article 80 (1) and, in addition to or instead of them, the NSA may impose an administrative fine in accordance with Article 83 of Regulation (EU) 2016/679 and under PDPA.

Where the complaint is obviously unfounded or excessive, the NSA may adopt a decision to dismiss the complaint.

The decision of the NSA is subject to appeal pursuant to the Administrative Procedure Code within 14 days of receipt.

The complaint to the Commission may be submitted by a letter, fax or by electronic means under the procedure of the Electronic Document and Electronic Trust Services Act. No action shall be taken on anonymous complaints and on complaints which are not signed by the complainant or by a legal or authorised representative.

It is not obligatory to bring the infringement before the NSA: the data subject may appeal against any actions or acts of the data controller and processor directly before the court pursuant to the Administrative Procedure Code.

The court is the only competent body to decide on compensation for the damage suffered as a result of an unlawful processing of personal data from the data controller or processor. The NSA are not authorised to issue decisions on that matter. So, if the data subject decides to bring her or his claim to the court directly, actually she or he saves time and procedural efforts.

But if once proceedings before the NSA have been started, the data subject may not bring a violation to the attention of the court.

Where a decision to implement a binding decision of the European Data Protection Board is required to be adopted, Articles 263 and 267 of the Treaty on the Functioning of the European Union shall apply accordingly.

Sanctions Under Art. 58 (2) of GDPR and Other Ones at National Level

There are not any special additional sanctions adopted by Bulgarian PDPA than fines and compulsory measures provided by GDPR.

The measures referred to in article 58 items (a) to (g) and (j) of GDPR and the measures referred to in article 80 (1) items 3, 4 and 5 are applicable to any violation of personal data protection. The specific measure, surely, depends on the background of the case in question and on the Commission's evaluation about the facts and their impact.

The national legislator differentiates the infringements which are subject to administrative fines or pecuniary sanction according to article 83 paragraphs 4 and 5 from certain other infringements which will be subject to a much lower fine that those in GDPR (article 86 PDPA: the size of the fine or pecuniary sanction is no more than BGN 5000, e.g. a bit more than EUR 2 500).

Even though PDPA does not provide it explicitly the practice of NSA shows that very often only a fine/pecuniary sanction or only a compulsory administrative measure (those under article 58 paragraph 2) is imposed by the Commission.

According to the Rules on the activity of the Commission, adopted in August 2019, the compulsory administrative measures under article 58 paragraph 2, article 80 paragraph 1 point 3, 4, 5 shall apply to: (i) consideration of a complaint against a personal data controller under Art. 38 of the PDPA; (ii) carrying out the control activity of the Commission under Art. 12 of PDPA including and when a signal is received; (ii) supervision of the commission under article 34, paragraph 4, article 42, paragraph 7, second sentence and article 43 of GDPR.

Damages for Intangible Harm – National Understanding and Practice

By the beginning of this century the national jurisprudence strictly followed the understanding that intangible harm is inherent only to individuals. Only in the last five–six years have the courts timidly started to recognize legal entities as entitled to bear intangible harms. But in both cases, individuals and legal entities, the intangible harms are calculated by the court only on the basis of "inner conviction" of the judge-rappoteur or of the panel. *"Inner convinction"* is one of the basic principles in making the decision according to our national law (art. 12 of Civil Procedure Code). There is not any methodology whatsoever, neither in a public legal act nor in any document meant for internal use of the judges to establish evaluation criteria. In a common mode the witnesses are those who "decide" the case: the only source of information about the emotions and negative consequences passed by the claimant are their (witnesses') statements. Usually, in such proceedings, only the claimant is allowed to summon witnesses about her/his emotions and non material consequences resulting from the wrong harmful activity of the respondent. Surely, the first step is to assert that there is something illegal done by the respondent. But once that fact is proved, the information of the possible harms comes from the witnesses. The Respondent witnesses are not allowed because of the understanding (the principle) that "the negative claims are not subject of proof". This way the respondent is deprived of the opportunity to rebut the testimonies of the claimant witnesses by other witnesses' testimony; the only step the respondent could rely on is the cross-examination.

Non-governmental Data Protection Options

In article 83 of PDPA the national legislator accepts the concept of article 80 of GDPR and provides the data subjects the right to mandate a not-for-profit legal person, which has statutory objectives which are in the public interest and is active in the field of protection of the rights and freedoms of natural persons with regard to the protection of their personal data, to lodge a complaint on his or her behalf and to exercise data subject rights. Such authorization does not concern the data subject right to receive compensation. With regards to the exercise of that right, the data subject may not mandate any other person or structure aforementioned.

There are certain hypothesis in PDPA when the data subject may exercise one's rights through the NSA or, respectively, through the Inspectorate. In such cases, the Commission or, respectively, the Inspectorate, shall verify the lawfulness of the refusal (Article 57 paragraph 1 PDPA).

Such hypotheses are the following:

(i) if the controller delays or refuses, in whole or in part, the provision of the information for processing grounds, storage period or criteria about it, which are the potential recipients of the data and/or other additional information, with the excuse that its delay or refusal is in order to avoid obstructing official or legal checks, investigations or procedures, avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protect public order and national security and/or protect the rights and freedoms of others;

(ii) if the controller restricts the access of the data subject to the data and information which concerns her or him and are under process with that controller, without any or with ungrounded explanation about such restriction;

(iii) if the controller refuses to proceed with rectification, completion, erasure or restriction of the processing of personal data because of any of the reasons in point (i) above or fails to inform the data subject about the refusal grounded on the same reasons;

In those cases, the NSA or, respectively, the Inspectorate, shall inform the data subject that at least all necessary verifications or consultations have taken place and of the right of the data subject to seek a judicial remedy (Article 57 paragraph 2 PDPA).

Data Protection Cooperation Between NSA and Other Regulators or Ombudsperson

The NSA regulates its activity, the activity of its administration, as well as administrative proceedings with Rules of Procedure promulgated in the *State Gazette.* (art. 9 par 2 PDPA). In those Rules (art. 14), in exercising its powers, the NSA is authorised and obliged to cooperate with state bodies and non-governmental organizations by participation in meetings of working groups, holding working meetings, carrying out joint activities, incl. inspections, implementation of joint projects and drafting regulatory acts. In the course of relations with other bodies and organizations, the NSA may conclude cooperation and mutual assistance agreements. Nowadays, the NSA has a very active cooperation with international structures such as Joint Supervisory Bodies and Working Parties to the EU Council and Data Protection Groups to the European Data Protection Supervisor.

What is National Security with Our Domestic Law and Administrative Practice

There is an explicit definition on "national security" in Bulgarian legislation. The law for the management and operation of the national security system, in its article 2, says: *"national security is a dynamic state of society and the state, while protecting the territorial integrity, sovereignty and constitutionally established order of the country, when the democratic functioning of the institutions and fundamental rights and freedoms of the citizens are guaranteed, as a result of which the nation preserves and increases its well-being and develops as and when the country successfully defends its national interests and realizes its national priorities".* This definition is applied to all the national laws which concern the national security though in different aspects: "National Security" Directorate Act, Classified Information Act, Special Intelligence Law, etc.

Practically, as of March 2015 when the Constitutional Court has repealed in whole the provisions of the Electronic Communication Act which had treated the obligation of the enterprises providing electronic communication services to store the traffic for a period of 12 months, our legislation provides for the unconditional application of Article 7 and 8 of the EC Charter, at least as regards the information that can be obtained from the electronic communications of any individual.

Where any information is required for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, a special permission should be issued by the court under the procedure of the Special Intelligence Act after a request by the competent authority: prosecutor's or investigator's offices.

Simeonov & Dermendjiev Law Firm, Sofia, Bulgaria