Home » Practice » Opinions of the CPDP for 2022 » Opinion of the CPDP regarding a request for preliminary consultation in connection with the development of a draft Ordinance on the functioning of the National Health Information System Opinion of the CPDP regarding a request for prior consultation in connection with the development of a draft Ordinance on the functioning of the National Health Information System OPINION OF THE COMMISSION FOR THE PROTECTION OF PERSONAL DATA reg. No. PNMD-01-67/2022, Sofia, 14.09.2022 REGARDING: Received request for preliminary consultation under Art. 36, par. 4 of Regulation (EU) 2016/679 in connection with the drafting of an Ordinance on the functioning of the National Health Information System. The Commission for the Protection of Personal Data (CPDP) in composition - Chairman: Ventsislav Karadzhov and members: Tsanko Tsolov, Maria Mateva and Veselin Tselkov, at a meeting held on 14.09.2022, considered a request with entry No. PNMD-01-67/08.07.2022 for preliminary consultation under Art. 36, par. 4 of Regulation (EU) 2016/679 in connection with the drafting of an Ordinance on the functioning of the National Health Information System (NHIS). The same was deposited by the Minister of Health, with a draft of the regulation, reasons for the same and a data protection impact assessment attached to it. In the reasons for the project, it is stated that according to the provisions of Art. 28d, para. 6 and para. 7 of the Health Law (HLA), the Minister of Health should issue an ordinance to settle the main issues related to the functioning of NHIS. It should be noted that the same includes the electronic health records of natural persons and incorporates registries, information databases and systems as defined by law. The reasons attached to the regulation state that they contain detailed information on the rules for operating the system, as well as specific data on the health status of the population. Additionally, information is provided that the regulation regulates the generation, content and maintenance of the electronic health record for natural persons. The same is a basic element in the functioning of the NHIS and is a structure containing a certain set of data on the activities performed by medical and non-medical specialists in medical and health facilities. The specified activities generate or use health information about individuals or are related to their health status. In addition to the above, the CPLD has been informed that rules have been introduced, according to which the registers, information databases and systems (defined in a normative act as being maintained by the Ministry of Health (MOH) and its subordinate budget administrators, by medical and the health facilities, from the NHIF and the insurance companies licensed under item 2 or under items 1 and 2 of section II, letter "A" of Annex No. 1 to the Insurance Code) are integrated into the NHIS. For greater clarity, in the reasons for the draft regulation, it is stated that the various relationships between users of the system, as well as the exchange of data with other registers, are regulated. In the documentation attached by the Ministry of Health,

goals are indicated that should be achieved through its introduction and exploitation by the persons authorized for this purpose: - helping to increase the quality and efficiency of the health care system by building an integrated health record of citizens, which includes all medical data from conducted treatment, therapies, medical research, administered medicinal products and other activities, which is a prerequisite for adequate diagnosis and effective treatment. Medical data is entered in real time. Citizens have the opportunity to track their data, including control if necessary. Patient service time is reduced; - helping to increase control in health care and reduce financial costs; - management and functioning of the health care system with the help of NHIS, which allows the monitoring of health care processes, the expenditure of financial resources and the making of effective management decisions based on data; - an opportunity to increase the quality of administrative services in health care. Taking into account the factual and legal complexity of the request, as well as the need to supplement the administrative file with a letter ex. No. PNMD-01-67#1/29.07.2022 according to the inventory of the CPLD, the following additional information is requested from the Ministry of Health: 1. The received opinions and comments of the interested parties within the framework of the public consultation held from April 7 to May 7, 2022 consultation of the draft Ordinance (in the part relating to the protection of personal data); and 2. The opinion of the data protection officer (DPO) of the Ministry of Health when performing the data protection impact assessment. By letter int. No. PNMD-01-67#2/09.08.2022 according to the inventory of the CPLD, the Ministry of Health sends the required opinions and comments, while regarding the requested opinion of the DLPD it informs that such was not expressed by the latter, as it was in the composition of the working group on the preparation of the draft regulation. However, they specify that the data protection impact assessment is agreed with it. Legal analysis: Modern technologies in health care can significantly improve the quality and access to health care, but only if their introduction corresponds to the requirements of the constantly developing legislation in this area and while respecting the fundamental rights and freedoms of citizens. The expectations are that technological development and digitization will improve the accountability of the health services offered, lead to innovative treatments and the development of new medical devices and medicines. On the other hand, digitization efforts in the field of health care will contribute to individuals being able to easily exercise control over their electronic health data, as well as to effectively exercise their rights related to the protection of their personal data. General conditions: The procedure for prior consultation with the supervisory body - CPLD is a special proceeding that develops according to the terms and conditions of Art. 36 of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). As a general rule, in order to improve compliance with the legal requirements for the protection

of personal data, when there is a possibility that the processing operations will lead to a high risk for the rights and freedoms of natural persons, the administrator is obliged to prepare the so-called data protection impact assessment to assess in particular the origin, nature, specificity and extent of this risk. The results of the performed assessment should be taken into account when determining the relevant measures to prove that the processing of personal data meets the regulatory requirements. Where the data protection impact assessment indicates that the processing operations lead to a high risk which the controller cannot limit with appropriate measures in terms of available technologies and implementation costs, before the start of the processing he should carry out a consultation with the supervisory authority. However, a preliminary consultation is also carried out in the special cases of Art. 36, par. 4 and par. 5 of the GDPR, namely when: a legislative or regulatory measure is drawn up that provides for the processing of personal data in order to ensure that the planned processing meets the requirements for the protection of personal data, and in particular to limit the risks associated with the data subject; as well as when national legislation requires controllers to consult the supervisory authority and obtain its prior authorization in relation to processing by a controller for the performance of a task carried out by it in the public interest, including processing in connection with social protection and the public health (precisely this hypothesis is provided for in Article 12, Paragraph 2 of the Personal Data Protection Act). In the present case, both special hypotheses are applicable, which require the MoH to consult with the CPLD in advance. According to the legal regulations, the preliminary consultation should be initiated before starting the processing of personal data, while in the present case the data is already being processed, since the National Health Information System (NHIS) has been functioning for more than a year and a half. In this case, the mandatory prior permission from the CPLD, which is a legal prerequisite for the actual commissioning of such information systems, is also missing. These circumstances necessitate the conclusion that the Ministry of Health (MOH), in its capacity as a personal data administrator, did not initially comply with the statutory requirements for the protection of personal data arising from the GDPR and the GDPR. This opinion is based solely on the circumstances stated in the request and therefore should not be understood as exhaustive and comprehensive. It does not limit the CPDP to consider any complaint or report related to its subject, and in a broader sense it does not affect its tasks and powers to supervise the activity of administrators and processors of personal data. According to the GDPR, the personal data controller alone or together with another controller determines the rules and procedures for data processing, which must comply with the personal data protection legislation. He must be able to prove this. For the data processing actions taken by the controller, joint controllers or the processor, both the

rules of accountability, transparency and good faith, as well as the norms relating to engaging in administrative criminal liability in relation to the legality of his/her personal data processing activities. For these reasons and on the basis of Art. 58, par. 3, b. a) in conjunction with Art. 36 of Regulation (EU) 2016/679 in conjunction with Art. 12, para. 2 of the Personal Data Protection Act, the Personal Data Protection Commission expressed the following OPINION: I. Principles: 1. The draft regulation does not comprehensively describe the objectives pursued with the introduction of the National Data Protection Regulation, which is a challenge to the clear, comprehensive and precise determination of the categories of data required for processing. There are no differentiated purposes for the primary processing of the data necessary for the provision of health services (assessment, maintenance or restoration of the health status of the individual), medical prescriptions, dispensing and provision of medicinal products and medical devices, including the provision of social security and administrative services or reimbursement services. The draft regulation also does not indicate whether the NHIS is used for the purposes of subsequent processing of personal data, such as: research on data and factors affecting health; electronic data of individuals generated in connection with the use of medical devices or applications; special registers related, for example, to a specific disease; health-related research, questionnaires and surveys, etc. The CPLD has information about the use of the NIS for such purposes from other files received in the last 2 years. The unclear definition of the goals is a prerequisite for distorting the assessment in relation to the roles and functions of the participants in the system. We recommend that the objectives of the system be comprehensively defined, clearly defining the objectives of the subsequent data processing, guaranteeing the rights of the data subjects. 2. The unclear definition of the purposes for processing in the draft ordinance leads to a lack of clear regulation regarding the roles and functions of the participants processing data through the system (administrators, processors, recipients of data, etc.). Their incorrect determination, in turn, leads to non-fulfillment of obligations related to the processing of personal data, such as providing information, guaranteeing the rights of data subjects, ensuring data security, performing a risk assessment and assessing the impact on data protection , the notification in the event of a data security breach, etc. The complexity and comprehensiveness of the system and its purposes precludes a single controller from being responsible for the processing of personal data in accordance with the requirements of Regulation (EU) 2016/679. 3. The draft regulation does not define the ways and means of providing information and ensuring transparency in the processing of personal data through the system in accordance with Art. 12, 13 and 14 of Regulation (EU) 2016/679, given that the information in question is different from that which is provided in connection with the provision of health care and medical assistance. The information should also include

the terms and conditions for the subsequent processing of the data in the NHIS. A standard for the provision of information should be defined, according to the requirements of Art. 12, 13 and 14 of Regulation (EU) 2016/679 for each specific purpose of processing, as well as for the subsequent exercise of rights by data subjects. 4. The draft regulation should take into account the operation of the Data Management Act (in force), as well as the discussion on a number of other European normative acts in the process of creation, such as the Artificial Intelligence Act, the Regulation on the European Health Data Space, etc. 5. Guaranteeing the rights of data subjects is a major concern of the regulation proposal. The reference to the general regime of Regulation (EU) 2016/679 for the exercise of rights does not take into account the specificity, objectives and complexity of the system. 6. The draft regulation does not take into account data protection requirements by design and by default, insofar as the regulation is developed with an already operational information system. 7. The draft regulation does not provide for measures and rules to regulate the order and obligations of the administrators to maintain the accuracy and completeness of the data in accordance with the principles proclaimed in Art. 5 of Regulation (EU) 2016/679. It is also not clear which is the leading one - the data from the NHIS or data from paper files. This also reflects on the exercise of rights by data subjects. 8. The draft regulation does not regulate the necessity and possibilities of data transfer to third countries or international organizations, as well as the conditions for this. In the context of data transfers, the system's data storage should also be taken into account. In view of the particular sensitivity and large volume of data, as well as in connection with the objective of the data subject exercising stricter control over his own data, it can be envisaged that the data from the NHIS is stored only in the EEA. In principle, the absence of such a requirement undermines control. 9. The draft regulation does not comprehensively regulate the rules for interoperability with other registers and databases with which the NIS is connected. They are not explicitly and exhaustively stated. 10. In addition, it should be noted that the acceptable assessment of the impact on the protection of personal data under Regulation (EU) 2016/679 should contain: a systematic description of the processing (Article 35, par. 7, letter a)): is taken taking into account the nature, scope, context and purposes of the processing (recital 90); the personal data, the recipients and the period for which the personal data will be stored are recorded; functional description of the processing operation; identifying the assets on which the personal data relies (hardware, software, networks, people, paper); possibly compliance with approved codes of conduct is taken into account (Article 35, paragraph 8); description of the technical means used to process personal data - this is absolutely necessary when performing the impact assessment, as it is also related to the "mobile application - mobile health record"; necessity and proportionality of the processing (Article 35(7)(b)):

the measures envisaged to comply with the Regulation (Article 35(7)(d) and recital 90 are defined, taking into account: the measures contributing to proportionality and necessity of the processing based on: [] specific, explicit and legitimate purposes (Article 5, paragraph 1, letter b); [] lawfulness of processing (Article 6); [] adequate, relevant and limited to the necessary data (Article 5, paragraph 1, letter c); [] limited duration of storage (Article 5(1)(e)); [] measures contributing to the rights of data subjects: [] information provided to the data subject (Articles 12, 13 and 14); [] right of access and portability (Articles 15 and 20); [] right to correction, erasure, objection, restriction of processing (Articles 16-19 and 21); [] recipients; [] processor(s) (Article 28); [] guarantees related to the international transfer(s) (Chapter V); [] prior consultation (Article 36). risk management for the rights and freedoms of data subjects (Article 35(7)(c)): the origin, nature, characteristics and gravity of the risks are assessed (see recital 84) or more specifically for each risk (unlawful access, unwanted modification and disappearance of data) from the point of view of data subjects: [] the sources of risks are taken into account (recital 90); [] the potential impacts on the rights and freedoms of data subjects are identified in case of illegal access, unwanted modification and disappearance of data; [] threats that can lead to illegal access, identification of unwanted modifications and disappearance of data; [] assessment of likelihood and severity (recital 90); [] the measures envisaged to deal with these risks are defined (Article 35, paragraph 7, letter d) and recital 90); stakeholder involvement: consultation with the data protection officer (Article 35(2); the opinion of the data subjects or their representatives is requested (Article 35, paragraph 9). II. Notes on substance: 1. In Art. 1, item 2 and item 3 of the draft ordinance states that it regulates the content and other information regarding the electronic health record of "citizens". We believe that, in view of legal clarity in relation to its application, it should be explicitly stated whether it is only a question of Bulgarian citizens or of foreign ones as well. 2. According to Art. 2 of the draft regulation NIS "can be used for the provision of administrative services". The subject of the regulation should be their comprehensive settlement, insofar as this will correspond to the principle of limitation of objectives (Article 5 of Regulation (EU) 2016/679). 3. According to Art. 6, para. 1 of the project "the module for maintaining a single environment for data exchange ... introduces ... rules ...". It should be borne in mind that the technological solution should fulfill the rules introduced by the regulatory framework. 4. In the context of Art. 9 of the proposal, it should be noted that the terms and conditions for keeping public and official electronic registers included in the NISIS are not provided for. 5. From the text of Art. 10 of the proposal does not make it clear how to ensure that all data is entered into the system with a high level of accuracy and completeness. 6. With regard to Art. 11 all internal-administrative services should be comprehensively arranged. 7. Pursuant to Art. 12 it should be noted that

system modules must function based on regulatory requirements and not on technical specifications. This is a direct consequence of the non-application of data protection principles by design and by default (Article 25 of Regulation (EU) 2016/679). 8. Regarding the individual authorization cited in Art. 13, para. 2, it is not clear on the basis of which document (introducing the relevant rules), the individual authorization of the specific persons is carried out. 9. In Art. 13, para. 3 of the project uses the term "medical documentation", and it is not clear whether it is identical to the term "health documentation", the legal definition of which is given in § 1, item 1 of the DR of ZZdr. 10. In Art. 13, para. 4 of the draft stipulates that "Electronic images of the results of imaging studies are also attached to the electronic health record, which are stored separately and are accessible upon prior request". The proposed text lacks clarity about who, under what conditions and in what order will be able to access the relevant electronic images of the results of imaging studies. 11. In paragraph 5 of Art. 13 of the project speaks of "consents of the person", and it is not clear whether these consents constitute "informed consent" in the sense of § 1, item 15 of the DR of the ZZdr or under Art. 28d, para. 2 of the Labor Code At the end of the same provision, it is foreseen that "other unstructured data will be collected and stored in the National Information System as an exception". It is not clear what these exceptions are, what are the prerequisites for their implementation, and whether they will contain the so-called "unstructured data" and personal data. 12. Throughout the text of the project, the use of different concepts (e.g. citizen/patient/person/natural person) makes an impression, with which, however, the aim is to refer to the same thing. Given the need to achieve legal certainty and predictability, it is advisable to harmonize the terminology used. 13. In Art. 14, para. 4 of the draft regulation, it is not clear whether the patient expresses consent or certifies with his signature. A clear distinction should be made between the two concepts, insofar as consent has direct implications for the rights and freedoms of the data subject and cannot be equated with authentication. 14. In Art. 15, para. 2 of the draft stipulates that the NIS will generate "a unique personal identification code (PIC) of the person in a format that does not allow the extraction of personal data from him". It should be noted that, by definition, unique identifiers linked to natural persons are in themselves personal data, as they can directly or indirectly identify a specific individual. In addition to the above in relation to Art. 15, para. 2, for the sake of legal certainty, we believe that the exact format should be specified in the text. 15. With regard to Art. 15, para. 3, item 1 of the draft regulation, the "identification data" should be specified. 16. In Art. 15, para. 4, item 9 of the draft stipulates that the patient's electronic health file will also contain "contact data with relatives" that can be accessed in emergency situations, but there is no description of the categories and types of data (e.g. name, phone number, etc.). In this sense, it is advisable to comprehensively provide for the same in

order to achieve legal certainty and transparency in their collection and storage. 17. We believe that the wording regarding the text of Art. 16, paragraph 1 of the draft would create ambiguity by using the expression "only at". With a view to clarifying it, we offer the following text: "After their creation, the maintenance of electronic health files of citizens in an up-to-date form is carried out by: ....". 18. In Art. 16, paragraph 3 of the project provides that the entries in the electronic health file will be able to be corrected by the medical or health facility that made the entry or by the person to whom it refers, by means of a request addressed to the system administrator, in this case – the Ministry of Health. "Certain cases" are also included, in which "up to 7 days after the generation of the health record, it is permissible to correct it by the medical or health facility that carried it out, on its initiative or at the request of the person to whom it refers", without however, to indicate who they are. Such wording leads to a lack of clarity and transparency for individuals regarding their right to correction. In the last sentence of Art. 16, paragraph 4 of the project states that the procedure for correcting health records will be approved by an order of the Minister of Health, which will be published on the health information web portal of the system www.his.bg. Given the fact that the rectification procedure is key to guaranteeing the rights and freedoms of data subjects, it should be an integral part of the regulation. At the moment, it cannot be analyzed within the framework of the initiated preliminary consultation with the CPLD, which in itself calls into question the effective exercise of the rights of data subjects. 19. In Art. 17, the proposed text "fifty-year period from the date of the person's death" for storing the electronic health record is extremely long and unfounded. In addition, the storage period should be defined in the Health Act, by analogy with the periods defined in the Accounting Act, the Tax-Insurance Procedure Code, the Labor Code, etc. Art. 17, para. 2 in connection with para. 3 of the draft regulation - the wording presented in this way does not make it clear whether the destruction of the data at a certain time and under what conditions is foreseen at all. The determination of storage periods and means of data protection is outside the subject area of competence of the CPLD. As a general rule, the same are determined by the personal data controller or by a regulatory act. Since significantly long periods of data storage are envisaged, the Ministry of Health, as the competent authority that proposes and adopts the regulation, should carry out a public interest analysis, as a result of which the appropriate, necessary and proportionate periods and mechanisms for the protection of the data corresponding to the pursued goals, such as pseudonymization, anonymization, encryption, etc. 20. In Art. 18, para. 5 of the project, the wording "legal access to registers of national importance" is too general and unclear. Even if such access is provided for by law, the specificity of the processed data and the levels of proportional access to such registers are not taken into account in the context of the NIS. These matters should

be expressly settled. In addition, "certain" service access to NHIS is used. We believe that it is necessary to specify the framework of this access, since the word "defined" implies a high degree of conditionality. 21. In Art. 19 of the project, the term "health data" is used instead of the legal term "health information" provided for in the LL. 22. Art. 20, para. 1 of the project states that "Valid, qualitative and up-to-date data is maintained in the NSIS". Taking into account the proclamations in Art. 5, par. 1, b. "d" of the GDPR principle of accuracy in the processing of personal data, the validity and quality of the data are characteristics that are directly related and placed depending on their relevance. In this sense, as long as the data is up-to-date, it should be both valid and qualitative, which is why we suggest dropping the last two characteristics. 23. In the context of Art. 22 with the regulation on NIS, the availability, integrity and confidentiality of the data processed through the system should be guaranteed. 24. In Art. 23, para. 1 of the draft Ordinance, a new item 2 should be added in the following sense: "maintaining the continuity of the system's work cycle"; 25. With regard to Art. 24, para. 2 of the project, it should be taken into account that the software products used are also subject to evaluation by the relevant administrators, monitoring the presence of personal data transfer through them. Questions arise about the presence of multiple personal data processors and subcontractors, which should be described comprehensively when providing the information under Art. 12, 13 and 14 of Regulation (EU) 2016/679. 26. In Art. 25, para. 1 of the draft stipulates that the NHIS "ensures the person's access to the data in the electronic health records in his electronic health record...". Here it should be borne in mind that in Art. 28d, para. 1, item 1 of the Civil Code refers to access to information, not data. For this reason, we encourage a terminological alignment with the concepts used at the law level. 27. Article 25, para. 3 introduces the concept of "service access" (Article 28 states "service purposes"), for which there is no definition. As can be seen from the provision, insurance companies are granted such access, which is contrary to recital (54) of Regulation (EU) 2016/679, as well as recital (19) of the Data Management Act. Again, the general phrase "legal access to registers of national importance" is used, which creates conditions for lowering the standards of protection in relation to the special categories of data that are processed through the NIS. In this regard, there are no accountability rules, for example, the maintenance of log files is regulated in Art. 30, para. 10 of the project, but the terms for their storage, purpose and control are not provided. Issues related to log files are directly related to the fair exercise of rights by data subjects and the controller's accountability. 28. In Art. 26, para. 3 of the project states that access is also provided through a mobile application "Mobile Health Record", which is another functionality of the system, which should have explicitly defined rules for the processing of personal data, which should take into account its specificity, as well as additional actors

such as app stores, mobile software and operating systems, tracking technologies such as location, etc. In addition, we believe that it should be described in more detail what means are provided for the indisputable identification of individuals using the "Mobile Health Record" application. 29. In Art. 26, para. 4 of the project, it should be specified whether only minors are covered (who, in the sense of the Law on Persons and Family, are persons from 14 years of age to 18 years of age) or whether minors (under 14 years of age) are also covered. In the event that both categories of persons are covered, the term "minors" should be replaced with "minors", which is traditionally used in the Bulgarian legal tradition. 30. The use of the individual's consent as a prerequisite for official access (e.g. by the NHIF and the state bodies for which access to registers of national importance is provided by law1) to his electronic health record raises the question of how these bodies and the institutions will exercise their tasks and powers in the absence or withdrawal of consent from the person. In addition, Art. 18, para. 5 and Art. 25, para. 3, item 3 provide that access to electronic health records for official purposes is also available to state bodies for which access to registers of national importance is provided by law. This means that they have the right of access on the relevant statutory basis - Art. 6, par. 1, letter c) of the GDPR "the processing is necessary to comply with a legal obligation that applies to the controller". Therefore, the administrator - Ministry of Health has a legal obligation to provide access to NIS to the state bodies to which the relevant law gives them the right to access registers of national importance. In connection with the above, the requirement to provide consent as a basis for processing personal data for official purposes of the relevant state bodies is in conflict with the provisions of the GDPR. The remarks also apply to the norms listed in Art. 28, para. 3 of the draft regulation. 31. In the first sentence of Art. 29 of the project provides that the consent can be changed or withdrawn. To the extent that this consent is identical to consent as a basis for processing personal data within the meaning of the GDPR, it should be borne in mind that consent under the GDPR can be given or withdrawn. Its "change" is not a term that is used in the GDPR and for this reason (in case it is applicable) we propose to make terminological consistency with the concepts used in the GDPR. 32. From the text of Art. 29, ex. 3 of the project, it is clear that there is no data that the principles of data protection were applied during design and by default (Article 25 of GDPR). These principles are fundamental in the development and functioning of information systems and databases of a similar type, such as the NZIS. In this sense, there is a lack of mechanisms to initially prevent the possibility of illegal storage of copies of patients' health records (such as prohibitions on copying, taking screenshots, etc.). The absence of such mechanisms creates extremely high risks for the rights, freedoms and interests of data subjects. 33. In Art. 30 of the proposal for an Ordinance, a new item 2 should be added, which provides for informing

individuals about the access made under para. 1 of the same article. In Art. 30, para. 10 of the project provides that the NIS will ensure traceability (audit log) of the actions of each user, listing the minimum details that will be saved: date/time of the action; system module in which the action is performed; action; object on which the action was performed; additional information and IP address. From the listed details, a question is raised regarding the so-called "additional information" - what is it and does it include personal data. An item that needs to be rethought. In addition, it is intended that users' IP addresses will be saved, which by definition fall within the scope of the concept of personal data. As the administrator of NHRIs, the Ministry of Health must introduce appropriate terms for their storage. In the event that these terms are not provided for in the regulation, they must be regulated in the internal rules and procedures of the Ministry of Health for the processing of personal data. 34. In Art. 31, para. 2 of the project, the term "anonymize" is used. A distinction should be made in which cases the data is anonymized, pseudonymized or restricted. In addition, from the wording thus presented, it can be concluded that non-anonymized data can be exchanged, which should be limited to "necessary". To define what is more precisely understood by "necessary". 35. In Art. 32, para. 4 regarding access to the Population Register - National Database "Population" the categories of data that need to be exchanged should be specified exhaustively. In para. 6 of the same article concerns the exchange of data with the Ministry of Internal Affairs "in the absence of legal obstacles to this". It should be borne in mind that the processing of special categories of data requires increased protection and the law must explicitly require or provide for such processing. 36. The systematic place of the provision of Art. 33 should not be in Section VII - Data Exchange. The disturbing thing in this text, and in other similar ones from the project, is that vocabulary is used that does not correspond to the Law on Normative Acts and Decree No. 883 of 04/24/1974 for its implementation. In the specific case, the expression "A functional module can be built in the system to collect information from..." is an example of bad practice under the normative regulation of an already functioning information system. 37. In Art. 34, para. 1 of the draft states that the personal data "are processed by the National Institute of Social Security...", while in para. 2 provides that the administrator of personal data in the system is the Ministry of Health. By its nature, NIS is a means of data processing, so the correct wording in this case would be: "processed through NIS". Pursuant to Art. 28d, para. 1 of the ZZdr MH creates, administers and maintains NZIS (provides the means for data processing), but it cannot be concluded that it is the only administrator of personal data in the system. This is also confirmed by para. 3 of Art. 34 of the project, according to which the medical and health facilities that enter, access or otherwise process personal data in the NHIS are independent administrators of personal data. Administrators of personal data

are also the bodies that keep registers, information databases and systems included in the NHIS if they collect such data. The above necessitates the conclusion that the Ministry of Health manages the system, but is not the only administrator of personal data in it. I.e. a distinction should be made between a system administrator and a personal data administrator. In Art. 34, para. 3 it is necessary to clarify the wording of the second sentence. The current wording leads to the conclusion that record-keeping authorities are controllers if and only if they collect personal data in the context of the regulation, not in principle. 38. According to para. 4 of Art. 34 of the project "When collecting and storing data in the NHIS, the privacy policy for the processing of personal data of the Ministry of Health is complied with, which for the purposes of this regulation is published on the website of the Ministry and on the health information web portal of the system www.his .bg". The privacy policy of the Ministry of Health cannot be binding on the other administrators of personal data in the system, unless they are joint administrators with the Ministry of Health. The specific rules for the processing of personal data through the NIS must be subject to regulation by the regulation itself in relation to all participants. 39. The analysis of para. 5 of Art. 34 of the project, requires the conclusion that the envisaged regime for exercising the rights of data subjects indicates the presence of the figure of joint administrators under Art. 26 of the GDPR, in the event that the relevant responsibilities of the administrators are defined in the legislation (see Art. 26, item 2 of the GDPR). The application of the conventional regime for the exercise of rights provided for in Art. 37b, para. 1 of the GDPR (by submitting a written application to the administrator), raises serious questions as to how far the administrators will be able to ensure the effective exercise of the rights of the data subjects, taking into account the fact that the NSIS has millions of users. In this sense, the achievements of technical progress allow the exercise of rights to be realized through actions in the user interface of the system (see Art. 37b, para. 3 of the LLPD), which contributes to the effective exercise of rights precisely in the cases of functioning of similar large-scale IT systems. 40. In Art. 36, para. 1 of the draft regulation, it is necessary to specify who and how determines the necessary professional qualities (job description, order of a superior, etc.). 41. In order to achieve greater clarity and in accordance with the requirements for the protection of personal data, we recommend the text of Art. 36, para. 2 of the project to be amended as follows: "The persons and authorities under Art. 13, para. 1 and Art. 18 do not have the right to access and use health information about individuals from the electronic health records and from the registers, information databases and systems included in the NHIS, for purposes other than those specified in this regulation." 42. In the text of Art. 40 of the project should provide terms for storage of the data recorded in the so-called system log (the comment under item 26 is applicable). 43. Regarding the proposed text of Art. 41 of the project, the

following should be taken into account: The obligation to maintain a register of processing activities under Art. 30 of the GDPR is the responsibility of the administrator or processor of personal data. In this sense, the "system" cannot support the intended registers. The register of processing activities serves for the accountability of the administrator and/or the processor, and the information it must contain is exhaustively specified in Art. 30, par. 1 and par. 2 of the GDPR. Keeping a register of processing activities is not the same as keeping a log of the actions performed by users in the information system. 44. After Art. 41 and before the Additional Regulations, a separate section should be provided for who carries out the control under this Ordinance and the manner of carrying it out. 45. In § 1, item 1 of the DR of the project, a legal definition of the term "anonymized" data is provided, which we propose to amend and supplement as follows: "Anonymized" means technically processed data with the aim of definitively and irreversibly eliminating the possibility to identify the entity to which they relate.46. With § 2 of the Transitional and Final provisions of the project, it is planned to give retroactive effect (ex tunc) to the rules for storage, access and maintenance of the electronic health records generated in the NHIS before the entry into force of the regulation.

It is well known that, in principle, general legal norms, including statutory legal norms, operate ex nunc. In modern legal systems, this principle is considered as a guarantee of predictability of the legal order and as an element of legal certainty. The idea underlying it is clear – that the addressees of the newly adopted legal norms can familiarize themselves with them and adapt their behavior to the patterns of behavior they establish. In jurisprudence, there is a permanent understanding that the retroactive effect of legal norms negatively affects legal certainty. In this regard, the Law on Normative Acts (LA) introduces explicit rules on the conditions under which normative acts can be given retroactive effect. In the specific case, the reverse action proposed in the draft ordinance is contrary to the rule of Art. 14, para. 2 of the ZNA, according to which retroactive force of a normative act issued on the basis of another normative act can be given only if the act on the basis of which it was issued has such force. The Health Law, as an act on the basis of which the regulation on the operation of the NHIS is issued, does not give such retroactive effect, therefore it is inadmissible for the latter to have such effect.

47. From the proposed text of § 3 of the Transitional and Final Provisions of the draft, it is not clear whether health documentation/information prepared before the entry into force of the regulation, nor from which period back in time, will be entered into the NHIS.

———————

1 See the hypothesis of Art. 28d of the Labor Code

CHAIRMAN:

MEMBERS:

Vencislav Karadjov /p/

Tsanko Tsolov /p/

Maria Mateva /p/

Veselin Tselkov /p/

Download files

Opinion of the CPLD regarding a request for preliminary consultation under Art. 36, par. 4 of Regulation (EU) 2016/679 in connection with the drafting of an Ordinance on the functioning of the National Health Information System.

print