Home »Practice» Opinions of the CPDP for 2019 »Opinion of the CPDP on issues related to determining the qualities" administrator "and" processor of personal data "in the relationship between insurance companies and medical institutions Opinion of the CPDP on issues related to the determination of the qualities of “administrator” and “processor of personal data” in the relations between insurance companies and medical establishments OPINION OF THE PERSONAL DATA PROTECTION COMMISSION Reg. : Request for an opinion on the determination of the qualities of administrator and processor of personal data. The Commission for Personal Data Protection (CPDP) composed of members: Tsanko Tsolov, Tsvetelin Sofroniev, Maria Mateva and Veselin Tselkov, at a meeting held on 09.01.2019, considered a request for an opinion / ent. № NDMSPO-01-1174 / 10.12.2018 / from “BSMC” Ltd., V., in connection with a case in determining the qualities of "administrator" and "processor" of personal data concerning the creation of a legal relationship with an insurance company, whose clients under insurance contracts to secure obligations, the medical center provides services, namely differentiated examinations and tests. The Medical Center is of the opinion that in its relations with insurers it acts as a processor of personal data. The letter points out that they have a dispute with one of the insurance companies, and the latter considers that the opinion of the CPDP (Reg. № NDMSPO-17-604 / 20.06.2018) on the case with the postal operator " C. ” AD and the medical center should have the capacity of personal data controller. The question is in what capacity (administrator or processor) the medical center should conclude a contract with the insurance company. Legal analysis: According to the legal definition referred to in Art. 4, item 7 of the General Data Protection Regulation (Regulation (EU) 2016/679) "controller" means a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means for the processing of data. personal data; where the purposes and means of such processing are determined by Union law or the law of a Member State, the controller or the specific criteria for determining it may be laid down in Union law or in the law of a Member State. The quality of administrator is a direct consequence of the fact that a particular person has chosen to process personal data for their own purposes or for purposes that are regulated by law. In this situation, except where legally required, the controller decides on the need to collect personal data, the categories of personal data, whether to change it during processing, where and how to use this data and with what the purpose of whether the data will be disclosed to third parties and what they will be, as well as for how long they will be stored, and when and in what way they will be destroyed. In addition, the Regulation imposes a certain range of obligations on the administrator. It must take appropriate technical and organizational measures relating to data security, taking into account the nature, scope, context and objectives of the data

processing, as well as the existing risks to the rights and freedoms of data subjects. In addition, according to the provision of Art. 30, para. 1 of Regulation (EU) 2016/679, the administrator shall maintain a register of the processing activities for which he is responsible. This commitment stems from the principle of accountability and the need for the administrator to be able to demonstrate at all times that he complies with the requirements set out in the Regulation. "Personal data processor" is "a natural or legal person, public authority, agency or body which processes personal data on behalf of the controller" (Article 4, item 8 of Regulation (EU) 2016/679). The main difference between the controller and the processor is that the latter does not act alone, but on behalf of the controller of personal data, ie. the consequences of the processing of personal data occur directly in the legal sphere of the controller. Their relationship is governed by contracts with another legal act under EU or Member State law, which regulates the subject matter and duration, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the rights and obligations of the controller, incl. . to carry out inspections (audits). The General Regulation also introduces specific obligations for the data processor, which are not limited to data security. For example, he is obliged to process personal data only on a documented order from the administrator / arg. Art. 28, para. 3, p. "A" in conjunction with Art. 29 of the General Regulation. In cases where it is necessary to appoint another data processor, this is done only with the express written permission of the controller. Like the administrator, according to Art. 30, para. 2 of the General Regulation, the processor also maintains a register of the processing activities for which he is responsible. In addition, for the sake of even greater clarity, the provision of Art. 28, para. 10 of the General Regulation explicitly provides that if the processor begins to determine the purposes and means of processing, he automatically begins to be considered an administrator. The principle of accountability referred to in Art. 5, para. 2 of Regulation (EU) 2016/679, requires participants in trade and civil turnover, taking into account their activities, to determine for themselves what is their legal relationship in relation to personal data processed by them - independent administrators, controller and processor within the meaning of Art. . 28 or joint administrators under Art. 26 of the General Regulation. Their choice should ensure not only formal but also substantive compliance with the requirements of Regulation (EU) 2016/679 and, accordingly, effective protection of the rights of data subjects. Also, it should be borne in mind that the provision of services, which usually exchange personal data between the contracting authority and the contractor, does not automatically lead to a relationship between administrator and processor within the meaning of Art. 28 of the Regulation. In principle, the controller may "entrust" a processor with processing activities for which he or she has the legal capacity to carry out, but for various organizational,

technical, financial or other reasons he or she has considered it more appropriate to carry out from the figure of the so-called processing. A classic example of outsourcing the processing of personal data to a processor is the obligation of the employer to provide services to employees of occupational health services. According to the provision of art. 2, para. 2 of Ordinance № 3 of 25.01.2008 on the terms and conditions for carrying out the activities of occupational medicine services, they are created by the employer within the enterprise or by independent legal entities or individuals registered under the Commercial Act, the Cooperatives Act or under the Non-Profit Legal Entities Act. Moreover, in para. 4 provides that when it is practically impossible for the employer to establish an occupational medicine service on his own, he shall conclude a contract with a service registered under Art. 25c of the Health and Safety at Work Act (OHSA). In this case, the activity of processing personal data in connection with inspections and research could not be carried out "on behalf" of the insurer (administrator), due to the fact that they can not be realized by him, but only by an organization having the quality of a “medical institution” within the meaning of the Medical Institutions Act. In addition, as evidenced by the provision of Art. 95, para. 1, item 2 of the Medical Establishments Act, the same may conclude contracts with insurers. These contracts should be concluded between the parties in their capacity as controllers of personal data, and not as a controller - processor within the meaning of Art. 28 of the General Regulation. The thesis expressed by the CPDP in its opinions on the qualities of "administrator" and "processor" in the postal and banking activities is similar, as they are published on its official website. On the other hand, and last but not least, the special legislation in the field of healthcare (legal and regulatory) provides for a number of obligations, measures, mechanisms, terms and conditions for protection of health information containing personal data that cannot be derogated from by contract. within the meaning of Art. 28 of the General Regulation. In view of the above and on the grounds of Art. 58, § 3, b. "B" of Regulation (EU) 2016/679, the Commission for Personal Data Protection expresses the following OPINION: 1. In this particular case, the activity of processing personal data in connection with the performance of examinations and tests could not be carried out on behalf of the insurer (administrator), due to the fact that they can not be carried out by him, but only by the organization, having the quality of "medical institution" within the meaning of the Medical Institutions Act. 2. The special legislation in the field of healthcare (law and by-laws) provides for a number of obligations, measures, mechanisms, order and conditions for protection of health information containing personal data, which cannot be derogated from by a contract within the meaning of Art. 28 of the General Regulation. 3. The participants in the trade and civil turnover, taking into account their activity, as well as the legislation applicable to it, should determine for themselves what are their legal relations in connection

with the personal data processed by them - independent administrators, administrator and processor within the meaning of Art. 28 or joint administrators under Art. 26 of the General Regulation. Their choice should ensure not only formal but also substantive compliance with the requirements of Regulation (EU) 2016/679 and, accordingly, effective protection of the rights of data subjects. which usually exchange personal data between the contracting authority and the contractor, does not automatically lead to a legal relationship between administrator and processor within the meaning of Art. 28 of the Regulation.

MEMBERS:

Tsanko Tsolov

Tsvetelin Sofroniev / p /

Maria Mateva / p /

Veselin Tselkov / p /

Downloads

Opinion of the CPDP on issues related to the determination of the qualities "administrator" and "processor of personal data" in the relationship between insurance companies and medical institutions

print