 Opinion of the CPLD on the figure of a data protection official in the context of the official relationship OPINION OF THE COMMISSION ON PROTECTION OF PERSONAL DATA reg. No. PPN-02-463/2021 Sofia, 18.11.2021 REGARDING: The figure of a data protection official in the context of the official relationship The Commission for the Protection of Personal Data (CPDP) in composition - chairman: Ventsislav Karadzov and members: Tsanko Tsolov, Maria Mateva and Veselin Tselkov, at a meeting held on 10.11.2021, considered a letter ent. No. PPN-02-463/04.10.2021 by a lawyer from the SAC, with which he asks the commission to establish whether and to what extent the Ordinance on the terms and conditions for evaluating the performance of employees in the state administration contradicts imperative rules and legal goals established by General Data Protection Regulation, and directly violates the statutory independence of a personal data protection official in the performance of his tasks. In connection with his request, the lawyer indicates reasons and notes on the applicable legal acts, expressing concern about a collision between them, as follows: Regulation (EU) 2016/679 of the European Parliament and of the Council introduced the figure of the data protection officer (GDPR). Its main functions are providing advice and consultation in the field of personal data protection, as well as supervising compliance with the Regulation in the administrator's organization. Article 39, paragraph 1 of the Regulation exhaustively specifies a mandatory minimum of tasks that the Data Controller must perform: - to inform and advise the administrator or processor of personal data and the employees who perform processing; - to monitor compliance with the regulation; - upon request, to provide advice regarding the data protection impact assessment and to monitor the performance of the assessment pursuant to Article 35; - to cooperate with the supervisory authority; - to act as a contact point for the supervisory authority. In order to guarantee the unhindered and independent exercise of these specific and statutory supervisory functions, the General Regulation contains the following imperative rules established in Art. 38, par. 3: The controller and processor of personal data shall ensure that the data protection officer does not receive any instructions for these tasks; and The Data Protection Officer cannot be dismissed from office, nor sanctioned by the controller or processor of personal data for the performance of their tasks. When the processing is carried out by a public body, the GDPR obliges it unconditionally to designate a data protection official, regardless of whether its main activities involve regular and/or large-scale processing of personal data - Art. 37, par. 1, b. "a". Probably, one of the reasons for this is that, in contrast to the commercial company, in the case of the public body, the pecuniary sanctions provided for in the Regulation would not have the same deterrent and disciplinary effect. Therefore, the

Regulation requires that the public authority is always assisted in monitoring internal compliance by a person with expert knowledge. In fulfillment of this requirement, by a decree of the Council of Ministers, the Classifier of positions in the administration was amended and supplemented, adding the position - personal data protection official for each type of administration. At the present moment, each Bulgarian administration, in fulfillment of its obligation under Art. 37, par. 1, b. "a" has appointed a personal data protection officer. For the most part, these persons are appointed to the civil service and have the status of civil servants. In this way, another specific legal relationship arising under the General Regulation is superimposed on the official legal relationship arising under the act of appointment and regulated by the Civil Servant Act - a legal relationship between the Administrator (Processor) of personal data and his DPLD. That is, a series of rights and obligations arise for both parties arising from two different sources - the Law on the Civil Servant and related secondary legal acts and Regulation (EU) 2016/679, the Personal Data Protection Act, and other legal acts in the field of data protection. Such a by-law is the Ordinance on the conditions and procedure for evaluating the performance of employees in the state administration. According to this regulation, the performance of each civil servant in the relevant administration is evaluated annually, including the data protection officer, if the same is appointed in a service relationship. Assessment has two components: achievement of pre-determined goals and demonstrated competencies. Based on the degree of achievement of the objectives and the demonstrated competences, the evaluating manager determines the annual assessment of the performance of the position, and this assessment further serves to determine the remuneration of the employees, for their promotion in rank, and in the case of an assessment of "unacceptable performance" may be a legal ground for termination of the employment relationship, that is, for the dismissal of the employee. Also, the regulation in question provides for the holding of interim meetings between the appraising manager and the appraised, which review the performance of the position, the competences shown by the employee, and specific actions to improve the performance can be noted. With the arguments presented in this way, the lawyer turns to the CPLD, considering that the "assessment of the performance of the position" held by the Data Controller and the "identification of specific actions to improve the performance" of the tasks of the Data Controller on the part of the Administrator (Processor), represents a legally established method of sanctioning and dismissal from office, as well as an opportunity to give instructions to the official on how to perform his tasks. In practice, the supervised person gives an assessment of the expertise of the person carrying out the supervision, and in case of an unsatisfactory assessment, imposes sanctions on him. In view of all the above, the lawyer asks the CPDP to establish whether and to what extent the

Ordinance on the conditions and procedure for evaluating the performance of employees in the state administration contradicts imperative rules and legal goals established by the General Regulation, and directly violates the statutory independence of a protection official of personal data in the performance of his tasks. In addition, the lawyer notes that the compromised autonomy of the official means the impossibility of independent supervision of the relevant public body, which in turn is a serious source of risk for the rights and freedoms of the data subjects. This risk increases many times in the conditions of a pandemic, when many Bulgarian public authorities carry out regular large-scale processing of special categories of data - those related to the health of both Bulgarian citizens and citizens of EU member states. The lawyer also requests that this letter be considered a signal under Chapter Eight, Section I of the APC, as well as requests to be promptly notified of the CPLD's decision on it. Legal analysis: This request contains fundamental questions regarding the application of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) in its part concerning the legal status of the data protection officer (DPO), which should be examined in accordance with Art. 57, par. 1, b. "c" in relation to Art. 58, par. 3, b. "b" of Regulation (EU) 2016/679. Since the request does not specify the information within the meaning of Art. 28, para. 1, item 4 of the Rules of Procedure of the Commission for the Protection of Personal Data and its Administration (PDKZLDNA), i.e. the person against whom the request was submitted is not specified, resp. on the same, proceedings cannot be instituted under Section II of the PDKZLDNA. According to consideration (97) and the provision of Art. 37, par. 5 of Regulation (EU) 2016/679, the administrator or processor of personal data should be assisted in monitoring internal compliance with the GDPR by a person with "expert knowledge and professional qualities" in the field of data protection law and practices. The legal framework listed in consideration (97) and the provision of Art. 37, par. 6 of Regulation (EU) 2016/679 defines the data protection officer as "employee" or "staff member". The grammatical interpretation of these concepts shows that the legislator had in mind specific natural persons, regardless of whether they are employees of the administrator or processor or employees of an external organization providing services in the field of personal data protection. The provision of Art. 37, par. 6 of Regulation (EU) 2016/679 allows the possibility for the Data Protection Authority to "perform tasks on the basis of a service contract". The logical interpretation shows that the Data Controller is not necessarily a party to the contract for the provision of the service. On the contrary, it should always be a specific employee performing the tasks arising from the contract. According to the provisions of Art. 37, par. 7, Art. 38, par. 4, Art. 39, par. 1, b. e) of Regulation (EU) 2016/679 the data protection officer is the point of contact for the data subjects, for the employees of the controller and for the supervisory authority. According to the

European Data Protection Board's Guidelines for Data Protection Officers ("DPOs"), "the purpose of these requirements is to ensure that data subjects (both inside and outside the organization) and supervisors will be able to easily and directly contact the Data Controller without having to contact another part of the organization". Direct contact with the Data Protection Authority is particularly important in the procedure for notifying the supervisory authority of a breach of personal data security within the meaning of Art. 33 of Regulation (EU) 2016/679, given the short 72-hour deadline for taking action and communication. This is an essential guarantee for the rights of data subjects on the one hand, and on the other hand it is a manifestation of compliance with the principle of accountability , laid down in the ORD.According to the provision of Art. 38, par. 3 of Regulation (EU) 2016/679 GDPR "cannot be dismissed from office" nor sanctioned by the administrator or processor of personal data for the performance of their tasks. Also, administrators/processors of personal data are required to ensure that the DPO "does not receive any instructions in relation to the performance of these tasks" and "reports directly to the highest management level of the administrator or processor of personal data".

"According to the GDPR, sanctioning is prohibited only if it is necessary as a result of the fulfillment of the obligations of the data controller in his capacity as a data controller. For example, the DPO may assess that a processing could lead to a high risk and advise the controller or personal data processor to carry out a data protection impact assessment, but the controller or personal data processor does not agree with the DPO's assessment. In such a case, the DLZD cannot be dismissed from office due to the fact that it gave this advice."1

With the norms of consideration (97) and Art. 38, par. 6 of Regulation (EU) 2016/679 outline the characteristic features of the DPO's position - "to perform his duties and tasks independently" and his functions "not to lead to a conflict of interest", regardless of whether the DPO is a member of the administrator's staff/ the processor, whether he is coordinating the position or performing tasks under a service contract. The clarifications made require that the Data Controller must be a person different from the controller/processor, as well as from the persons who determine the purposes and means of personal data processing at the respective controller/processor (such as the manager, chief executive officer, chief operating officer, chief financial officer, Chief Medical Officer, Head of Marketing, Head of Human Resources or Head of IT, but also other functions further down the organizational structure if the positions or functions in question are related to determining the purposes and means of processing of the data).

An essential element of the independence of the Data Controller is that it "reports directly to the highest management level of

the administrator or processor of personal data" (Article 38, Par. 3 of the GDPR). This provision gives a clear signal that when the Data Controller is an employee of the controller/processor, including when he is a public body, his position should be organizationally and functionally separated from the other structural units of the organization. Analogous examples of positions in the administration that directly report their activity to the highest management level are the positions of information security officer and financial controller. As a rule, these positions are directly subordinated to the head of the respective organization, i.e. functional management of their activity cannot be mediated through their structural positioning within the administrative units (directorates, departments, sectors). Even when the DPO fulfills this function by reconciliation or by assignment to another position held, the DPO is subject to an assessment carried out by the relevant direct supervisor, who in this case, in order to fulfill the condition of the GDPR, is the head of the organization. This understanding fully corresponds to the requirements of Art. 4, para. 1 of the Ordinance on the terms and conditions for evaluating the performance of employees in the state administration, in which it is stated that the evaluator is the manager to whom the relevant employee is directly subordinate - in this case the DLZD must be evaluated, as a civil servant holding the post of DLZD according to The classifier of positions in the administration directly from the appointing authority.

In conclusion, it can be summarized that the GDPR provides several guarantees that enable the data controller to act independently:

• no instructions are given by the administrators or personal data processors regarding the performance of the tasks of the Data Protection Officer;

• it is not allowed to dismiss the administrator in connection with the performance of the tasks of the Data Controller;

• no conflict of interest with any other tasks and duties is allowed.

However, this does not mean that the GDPR is unaccountable, uncontrollable and unaccountable to the administrator/processor, including when it is a public body. In this sense, the mechanism for evaluating the activity of the civil servant holding the position of DPO, provided in the Ordinance on the conditions and procedures for evaluating the performance of employees in the state administration, does not directly contradict the requirement for accountability and independence under Regulation (EU) 2016/679 of the DPO to the highest management of the public body. Moreover, the GDPR requires that the Data Controller be independent in the performance of the assigned tasks within the meaning of Art. 39, as it bears no personal liability under the GDPR in case of non-compliance with data protection requirements. The

administrator or processor of personal data is the one who is obliged to guarantee and be able to prove that the processing is carried out in accordance with the GDPR. Compliance with data protection regulations is the responsibility of the controller or processor of personal data. At the same time, the DLZD may bear disciplinary responsibility under the general rules, for example, violation of labor discipline, in case of theft, physical, psychological or sexual harassment or similar gross manifestations of behavior incompatible with labor discipline, etc.

For these reasons and on the basis of Art. 58, par. 3, b. b) from Regulation (EU) 2016/679 in conjunction with Art. 10a, para. 1 of the Personal Data Protection Act, the Personal Data Protection Commission expresses the following

OPINION:

The mechanism provided for in the Ordinance on the terms and conditions for evaluating the performance of employees in the state administration, the mechanism for evaluating the activity of the civil servant occupying the position of DLPD, does not contradict the requirement for independence of DLPD under Art. 38, par. 3 of Regulation (EU) 2016/679.

CHAIRMAN:

MEMBERS:

Vencislav Karadjov /p/

Tsanko Tsolov /p/

Maria Mateva /p/

Veselin Tselkov /p/

1 Guidelines for Data Protection Officers ("DPO") adopted on 13 December 2016, last revised and adopted on 5 April 2017.