Home »Practice» Opinions of the CPDP for 2021 »Opinion of the CPDP on signing documents by an administration with a qualified electronic signature and providing them in an electronic environment Opinion of the CPDP on signing documents by an administration with a qualified electronic signature and providing them in an electronic environment OPINION OF THE COMMISSION FOR PERSONAL DATA PROTECTION Reg. № PNMD-01-11 / 2021 Sofia, 17.06.2021 SUBJECT: personal data (CPDP) composed of - Chairman: Ventsislav Karadzhov and members: Tsanko Tsolov, Maria Mateva and Veselin Tselkov, at a meeting held on 09.06.2021, considered a request for an opinion with ent. № PNMD-01-11 / 2021 by the Ministry of Education and Science (MES), which addresses the issue of signing documents by employees in the administration with a qualified electronic signature (QES) and providing them in an electronic environment for the purposes of document flow. The Ministry of Education and Science informs that according to the requirements of the Ordinance on General Requirements for Information Systems, Registers and Electronic Administrative Services (NIISREAU) they are obliged to use an electronic document management system and participate in electronic exchange of documents with other administrations. carrier, except in cases where this is determined by law. Pursuant to Art. 37 of NOIISREAU electronic documents are signed with an electronic signature issued under the Ordinance on electronic signature certificates in administrations. Electronic signing is also established with regard to the result of the provided electronic administrative services (Article 9 of the NIISREAU). In Art. 101, para. 3 of the Ordinance on the Exchange of Documents in the Administration (NODA) also regulates the preparation of electronic documents to be signed with an electronic signature. In this regard, an analysis is presented, according to which certification service providers include information about PINs in qualified certificates for qualified electronic signatures (KUKEP). However, there are concerns that this information is visible both in qualified certificates for qualified electronic signatures issued to individuals (in their personal capacity) and in KUKEP, which are issued to individuals associated with legal entities. ie in official capacity). The concerns relate to the fact that when sending a signed document with an electronic signature without changing its format (for example, by scanning the document or converting it to another format), all those who have access to the document can receive both data, necessary for validation of the electronic signature, validity period and data for the administration (name / UIC / BULSTAT), as well as personal data for the person who signed the document - three names and PIN, as well as e-mail address contained in the electronic signature. In view of the above, the Ministry of Education and Science considers that there are no normative grounds for granting access to the personal identification number to individuals acting in the performance of their official duties, resp. there is also a lack of compliance with regulatory

requirements for personal data protection. In this regard, the Ministry of Education and Science appealed to the CPDP with a request to express an opinion on the case. For these reasons and taking into account the supervisory powers of the Communications Regulation Commission (CRC) in the field of legislation governing electronic certification services, the CPDP sent an official request with ref. № PNMD-01-11 # 1 / 22.03.2021. The following question is asked in it: “It is indisputable that the PIN is necessary for the issuance of QES (Article 43 of the Electronic Document and Electronic Certification Services Act), but there are Is there an explicit normative requirement for the PIN of the QES holder to be visible when signing electronic documents for an unlimited number of persons - recipients of the documents in question? ” In response to the question posed, with his letter with ent. № PNMD-01-11 # 2 / 28.05.2021, CRC provides the following information: "… according to the current legislation in the field of electronic certification services there is no such regulatory requirement." Legal analysis: In the provision of art. 3 of Regulation (EU) № 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and certification services for electronic transactions in the internal market and repealing Directive 1999/93 / EC (Promulgated L OJ 257 of 28 August 2014) the legal definitions of the terms related to the case under consideration are as follows: According to item 10) "electronic signature" means data in electronic form that are added to other data in electronic form or are logically related to them, and which the holder of the electronic signature uses to sign; According to item 11) "advanced electronic signature" means an electronic signature that meets the requirements set out in Article 26; According to item 12) "qualified electronic signature" means an advanced electronic signature, which is created by a device for creating a qualified electronic signature and is based on a qualified certificate for electronic signatures; According to item 13) “electronic signature creation data” means unique data used by the electronic signature holder for the creation of an electronic signature; According to item 14) “electronic signature certificate” means an electronic certificate, which connects the data for validation of an electronic signature with a natural person and confirms at least the name or pseudonym of this person; According to item 15) "qualified electronic signature certificate" means a certificate for electronic signatures issued by a provider of qualified certification services and meeting the requirements set out in Annex I; According to item 16) "certification service" means an electronic service, usually provided for remuneration, which consists of: a) the creation, verification and validation of electronic signatures, electronic stamps or electronic time stamps, electronic registered mail services and certificates related to these services; or (b) the creation, verification and validation of certificates of authenticity on a website; or (c) the storage of electronic signatures, stamps or certificates relating to these services. According to Annex I of Regulation (EU) 910/2014,

qualified electronic signature certificates should contain a specific set of data regarding holders. However, the key is the distinction between the purposes for which this data is processed - the issuance and use of the electronic signature. By virtue of Art. 24, para. 1 of Regulation (EU) 910/2014, when issuing a qualified certification service certificate, the qualified certification service provider shall verify by appropriate means and in accordance with national law the identity and, if applicable, all specific data of the natural or legal person to whom the qualified certificate is issued. This information shall be verified by the qualified certification service provider directly or through a third party in accordance with national law: (a) through the personal presence of the natural person or an authorized representative of the legal person; or (b) remotely by means of electronic identification, for which the physical presence of the natural person or an authorized representative of the legal person has been ensured prior to the issuance of the qualified certificate and the device in question meets the requirements of Article 8 in terms of security levels. significant ”or“ high ”; or (c) by a certificate of qualified electronic signature or qualified electronic seal issued in accordance with point (a) or (b); or (d) using other nationally recognized identification methods that provide a level of security equivalent to physical presence in terms of reliability. The equivalent level of assurance shall be confirmed by a conformity assessment body. This provision obliges the certification service provider to unquestionably identify the holders of an electronic signature by collecting and processing a certain amount of personal data for this purpose. Undoubtedly, one of the ways to identify the data subject is to process his / her PIN together with other identification data. However, this does not mean that the PIN should be visible when signing documents. The main objective in the use of the services regulated by Regulation (EU) 910/2014 is to ensure the provision of secure electronic identification and secure electronic authentication. These obligations are explicitly imposed on the providers of electronic certification services and therefore there is neither a need nor a legal basis for the PIN of the holder to be visible to an unlimited number of persons - participants in the exchange of electronic documents. The provision of Art. 11 of the Civil Registration Act (CRA) states that the PIN is an administrative identifier through which individuals are uniquely identified. In this regard, the PIN can be normatively established as a prop, which e.g. is part of an application that the person submits in connection with a request to initiate administrative proceedings or to provide a service. In such cases, the purpose and grounds for processing the PIN are provided in a normative act and it is part of the content of a specific document and not the electronic signature. Moreover, according to Art. 25, para. 2 of Regulation (EU) 910/2014, the legal force of a qualified electronic signature is equivalent to that of a handwritten signature, the validity of which does not require the addition of a PIN. For these reasons and on the grounds

of Art. 58, para. 3, p. "B" of Regulation (EU) 2016/679 in conjunction with Art. 10a, para. 1 of the Personal Data Protection Act, the Commission for Personal Data Protection expresses the following OPINION: 1. According to the current legislation in the field of electronic certification services, there is no regulatory requirement and legal basis of electronic documents.2. Taking into account the above in item 1, the Ministry of Education and Science should turn to the provider who provided the relevant electronic certification services, in order to take action to suspend the visualization of the PIN of the QES holder when signing electronic documents by employees administration.

THE CHAIRMAN:

MEMBERS:

Ventsislav Karadzhov

Tsanko Tsolov

Maria Mateva / p /

Veselin Tselkov / p /

Downloads

Opinion of the CPDP on signing documents by an administration with a qualified electronic signature and providing them in an electronic environment

print