Home »Practice» Opinions of the CPDP for 2018 »Opinion of the CPDP on rules for non-bank financial institutions for unambiguous identification of individuals in a virtual environment when providing financial services at a distance Opinion of the CPDP on rules for non-bank financial institutions for unambiguous natural persons in a virtual environment when providing financial services at a distance OPINION OF THE COMMISSION FOR THE PROTECTION OF PERSONAL DATA Reg. № NDMSPO-01-264 / 2018 Sofia, 22.11.2018 SUBJECT: Rules for non-bank financial institutions for unambiguous identification of individuals in a virtual environment when providing financial services at a distance Commission for Personal Data Protection (CPDP) , Commission) composed of: members: Tsvetelin Sofroniev, Maria Mateva and Veselin Tselkov, at a meeting held on 21.11.2018, considered a file with registration № NDMSPO-01-264 / 2018 by Mr. P.D. . - Manager of "B.F. Ltd., on issues concerning rules for non-bank financial institutions for unambiguous recognition of individuals in a virtual environment when providing financial services from a distance. ,, B.F. “Ltd. is a non-bank financial institution, entered with registration № ****** in the Register of Financial Institutions under Art. 3a of the Credit Institutions Act (CIA) of the BNB. The company provides financial services at a distance and in particular consumer loans to individuals. The application and granting of loans to consumers is carried out in absentia in accordance with the Law on the Provision of Distance Financial Services and the Law on Consumer Credits. The legal statements when applying for and granting loans to individuals are exchanged and certified by an advanced electronic signature under Art. 13, para. 2 and para. 4 of ZEPEUU, created by means of individualization - telephone and e-mail, together with personal code, which are given the meaning of a handwritten signature on the related electronic statements. As a financial institution, the company is among those who must implement measures to prevent money laundering and terrorist financing. However, some of the loans are small amounts, the values of which are significantly below the thresholds requiring special identification measures under the LMML and the LMFTA. In carrying out the activities of the financial institution, practical difficulties are identified related to the unambiguous separation of one person from another in a virtual environment. Even if control and verification of the identification data provided by the client is performed, the risk of requesting and using financial services by individuals through the so-called "Identity theft" when one person impersonates another. The Electronic Identification Act aims to regulate public relations related to the electronic identification of individuals, but its entry into force has been postponed to January 1, 2019. Currently, the legal and economic environment in which non-banking financial institutions operating remotely consumer lending services to individuals remains uncertain and threatened by non-specific non-market risks. Objective difficulties in unambiguously recognizing individuals in a virtual

environment are a prerequisite for fraud and other forms of illicit behavior by unscrupulous individuals, which require special measures not to undermine the credibility and economic efficiency of lending to non-bank financial institutions. At the same time, in order to comply with the requirements of Regulation (EU) 2016/679 (GDPR), non-bank financial institutions must minimize the collection and processing of personal data of individuals, in accordance with the objectives of the services provided. The processing of a larger volume of users' personal data in order to protect the economic interests of the controller may infringe the principle of proportionality in the processing. The above aims to justify the need for an opinion of the Commission for Personal Data Protection on the following issues: - In the application of Regulation (EU) 2016/679 (GDPR) of 25 May 2018, does the opinion expressed in Decision remain relevant and applicable? № Ж-39 / 09.06.2016 p. of the CPDP for the fact that a non-banking financial institution, as a controller of personal data, is obliged to identify the client or verify it, to require an official identity document containing his photo, what document is the ID card, and to make a copy of it and store it for five years. - Upon establishing that a natural person has applied for and / or received a cash loan under the Law on the Provision of Distance Financial Services from a Non-Bank Financial Institution, through the so-called "Identity theft" where one person pretends to be another, is the non-bank financial institution, as a controller of personal data, obliged to notify the supervisory authority of personal data breaches in accordance with the requirements of Article 33 of Regulation (EU) 2016 / 679 (GDPR). In this regard, Mr. PD asks the CPDP to express an opinion and instructions addressed to financial institutions on the processing of personal data of individuals in the provision of financial services at a distance, in order to overcome the specific risks associated with unambiguous differentiation of individuals in a virtual environment. Legal analysis: The Credit Institutions Act (CIA) defines the activities and inherent obligations of banking and non-banking financial institutions. Non-bank financial institutions within the meaning of Art. 3, para. 1 of the LCI have the right to carry out as main activity the acquisition of shares in a credit institution or other financial institution, granting loans with funds not raised through public attraction of deposits or other repayable funds, performing payment services within the meaning of the Act for payment services and payment systems (ZPUPS), etc. Until the entry into force of Art. 100, para. 1 of the PDPA, by virtue of the Final Guidelines on the Security of Internet Payments of the European Banking Authority, the financial institution must conduct in-depth authentication of the customer in order to authorize online payments by the customer and to issue or modify electronic direct debit mandates. In the context of the delegated Commission Regulation supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council as regards regulatory technical standards for in-depth identification of customers and

common and secure open standards of communication, identification requirements are significantly increased, especially when the customer performs an action at a distance, which could lead to a risk of payment fraud or other abuse. Within the meaning of item 63 of the Additional Provisions of the PDPA, the establishment of identity is "a procedure that allows the payment service provider to verify the identity of the payment service user, including the use of personalized security features of the user." Apart from the obligations imposed in order to carry out the activities of the financial institution, the Anti-Money Laundering Measures Act (AMLPA) defines the measures for prevention of the use of the financial system for money laundering purposes, as well as the organization and control over their implementation. In Art. 3 of the LMML, the measures for prevention of the use of the financial system for the purposes of money laundering are outlined and they are: 1. complex inspection of the clients; 2. collection and preparation of documents and other information under the conditions and by the order of this law; 3. storage of the documents, data and information collected and prepared for the purposes of this law; 4. assessment of the risk of money laundering; 5. disclosure of information regarding suspicious operations, transactions and clients; 6. disclosure of other information for the purposes of this law; 7. control over the activity of the obligated subjects under Section II of this Chapter; 8. exchange of information and interaction at national level, as well as exchange of information and interaction between the Financial Intelligence Directorate of the State Agency for National Security, the financial intelligence units of other countries and jurisdictions, as well as with the competent authorities in the relevant field and organizations in other countries. The above-mentioned measures for prevention and control of their implementation are obligatory for the subjects listed in Art. 4 of the same law. In Art. 4, para. 1, the Bulgarian National Bank and the credit institutions operating on the territory of the Republic of Bulgaria within the meaning of the Credit Institutions Act are marked as obligated entities. ,, B.F. “Ltd. is a non-bank financial institution, entered with registration № ****** in the Register of Financial Institutions under Art. 3a of the Credit Institutions Act (CIA) of the BNB, therefore the company, falls within the scope of the obligated entities under Art. 4, para. 1 of the LMML. With the LMML for certain legal entities for which obligations for taking measures for prevention are envisaged, in particular - actions for identification of clients and verification of their identification (Art. 3, para. 1, item 1 of the LMML). In the provisions of Chapter V of the LMML, namely in Art. 52 and Art. 53 reflects that Customer identification and verification of identification is performed using documents, data or information from a reliable and independent source. The way of identifying the clients and checking their identification is determined. For natural persons it is required to present an official identity document and register its type, number, issuer, as well as the name, address, unique civil number, and for

natural persons having the status of sole trader - and by presenting documents identifying it in its commercial capacity. According to Art. 53, para. 1 of the LMML - The identification of natural persons is carried out by presenting an official identity document and taking a copy of it. Therefore, the employees of the financial institution take a copy of the ID card during the initial visit to the non-banking financial institution, after which they have to verify the authenticity of the data provided by the person, and not every time to take a new copy or re-scan the ID card. According to Art. 53, para. 2 in the identification of natural persons shall be collected data for: 1. the names; 2. the date and place of birth; 3. official personal identification number or other unique element for establishing the identity, contained in an official identity document, the term of validity of which has not expired and on which there is a photo of the client; 4. any citizenship that the person holds; 5. country of permanent residence and address (mailbox number is not sufficient). When entering into a business relationship, data on the person's professional activity and the purpose and nature of the person's participation in the business relationship are collected by using documents, data or information from a reliable and independent source, completing a questionnaire or other appropriate means. Based on the risk assessment under Chapter Seven of the Act, namely in connection with clarifying the origin of the funds, the persons under Art. 4 may collect additional data under the conditions and by the order of the regulations for application of the law. When the official identity document does not contain all the data under para. 2, the collection of the missing data shall be carried out by presenting other official identity documents or other official personal documents, the validity of which has not expired and on which there is a photo of the client, and taking a copy of them. In the absence of another possibility, the collection of data under para. 2, items 3 and 5 may also be performed by presenting other official documents or documents from a reliable and independent source. Where identification is carried out without the presence of the identifiable natural person, identification may also be carried out by presenting a copy of an official identity document. In these cases the verification of the collected identification data shall be carried out by the order of art. 55, para. 2. The customer identification procedure is mandatory for non-bank financial institutions. In Art. 2, para. 1 of the Regulations for application of the Law on Measures against Money Laundering it is stated that this is done by presenting an official identity document and taking a copy of it, and in para. 3 are exhaustively listed the data to be collected: 1. the names; 2. the date and place of birth; 3. official personal identification number or other unique element for establishing the identity, contained in an official document, the term of validity of which has not expired and on which there is a photo of the client; 4. citizenship; 5. country of permanent residence and address (mailbox number is not sufficient). Chapter III of the LMML sets out the terms of storage of information

and statistical data. The provisions of Art. Art. 67, para. 1 states that the persons under Art. 4 (in the specific case the non-bank financial institutions) shall keep for a period of 5 years all documents, data and information collected and prepared in accordance with this Act and the regulations for its implementation. In the cases of establishing business relations with clients, as well as in the cases of entering into correspondent relations, the above-mentioned term begins to run from the beginning of the calendar year following the year of termination of the relations. According to Art. 4, para. 7 of Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) "controller" means a natural or legal person, public authority, agency or another structure, which alone or together with others determines the purposes and means for the processing of 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. As an administrator of personal data within the meaning of Art. 4, para. 7 of the General Regulation, the non-banking financial institution (BF OOD) has an obligation to process the personal data of individuals in cases where this is permissible. The processing of personal data in this case meets the requirements of Art. 6, para. 1 (c) of the General Data Protection Regulation, namely processing is necessary to comply with a legal obligation to which the controller is subject. The processing of personal data by the financial institution should be carried out in compliance with the principles listed in Chapter II of the Regulation, Art. 5 - personal data must be: processed lawfully, in good faith and in a transparent manner with regard to the data subject ("lawfulness, good faith and transparency"); collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, for scientific or historical research or for statistical purposes shall not be considered, in accordance with Article 89 (1), incompatible with the original objectives ("limitation of objectives"); appropriate, related to and limited to what is necessary in relation to the purposes for which they are processed ("data minimization"); accurate and, if necessary, kept up to date; all reasonable steps must be taken to ensure the timely erasure or correction of inaccurate personal data, taking into account the purposes for which they are processed ("accuracy"); stored in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept for a longer period, provided that they are processed solely for archiving purposes in the public interest, for scientific or historical research or for statistical purposes in accordance with Article 89 (1), provided that appropriate technical and organizational measures provided for in this Regulation in order to guarantee the rights

and freedoms of the data subject ("storage restriction"); processed in a way that ensures an adequate level of security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, applying appropriate technical or organizational measures ("integrity and confidentiality"). Regarding the second question raised in the request, namely when establishing that a natural person has applied for and / or received a cash loan under the Law on the Provision of Distance Financial Services from a Non-Bank Financial Institution, through the so-called "Identity theft", when one person pretends to be another, is the non-bank financial institution, as a personal data controller, obliged to notify the supervisory authority of personal data breach in accordance with the requirements of Art. 33 of Regulation (EU) 2016/679 (GDPR), the same violation poses a risk to the rights of individuals. Art. 33 of the General Data Protection Regulation should be considered in conjunction with recital 85, namely that breaches of personal data security may, if not adequately and timely addressed, lead to physical, material or non-material damage. for individuals, such as loss of control over personal data or restriction of their rights, discrimination, identity theft or fraud with false identity, financial losses, unauthorized removal of pseudonymization, damage to reputation, breach of confidentiality of personal data protected by professional secrecy, or any other significant economic or social adverse consequences for the individuals concerned. Therefore, as soon as it identifies a breach of personal data security, the controller should notify the supervisory authority of the personal data breach without undue delay and, where practicable, no later than 72 hours after learning of it, unless the controller is unable to demonstrate in accordance with the principle of accountability that the breach of personal data security is not likely to jeopardize the rights and freedoms of individuals. Where such notification cannot be given within 72 hours, it shall state the reasons for the delay and that the information may be provided in stages without undue further delay. In connection with the above and on the grounds of Art. 58, para. 3 of the General Data Protection Regulation, the Commission for Personal Data Protection expressed the following OPINION: Non-banking financial institutions, such as data controllers, are obliged to require an official identity document containing his photo, which document is an identity card, as well as to make a copy of it and keep it for five years (Article 67, paragraph 1 of the LMML). The obligation is according to art. 53, para. 1 of the Law on Measures against Money Laundering, namely the identification of natural persons is carried out by presenting an official identity document and taking a copy of it. When it is established that a natural person has requested and / or received a cash loan under the Law on the Provision of Distance Financial Services from a Non-Bank Financial Institution, through the so-called "Identity theft", when one person impersonates another, an obligation of the non-bank financial institution, as a

controller of personal data, to notify the supervisory authority of a breach of personal data security in accordance with the requirements of Art. 33 of Regulation (EU) 2016/679 (GOPR). The breach of personal data security may pose a risk to the rights and freedoms of individuals, therefore, as soon as it finds a breach of personal data security, the controller should notify the supervisory authority of the personal data breach without undue delay and where practicable, no later than 72 hours after learning of it (recital 85 of the Regulation). It is also the data controller's responsibility to notify the data subject of a breach of the security of his or her personal data the provisions of Article 34 of the General Regulation).

MEMBERS:

Tsvetelin Sofroniev / p /

Maria Mateva / p /

Veselin Tselkov / p /

Downloads

Opinion of the CPDP on rules for non-bank financial institutions for unambiguous recognition of individuals in a virtual environment when providing financial services at a distance

print