



БЪЛГАРСКА  
НАРОДНА БАНКА

**Насоки**  
**за дистанционно установяване на делови взаимоотношения с клиенти на**  
**банки**

Кредитните институции следва да съобразят настоящите насоки при извършване на дистанционно установяване на делови взаимоотношения с клиенти.

Настоящите Насоки са приети от Управителния съвет на Българската народна банка на основание чл. 108, ал. 6, т. 1, б. а от Закона за мерките срещу изпирането на пари, чл. 73, ал. 4, във връзка с ал. 1, т. 11 от Закона за кредитните институции и Решение на УС на БНБ за прилагането на Насоки на ЕБО (EBA/GL/2022/15) относно използването на решения за дистанционно установяване на делови взаимоотношения с клиенти, съгласно член 13, параграф 1 от Директива (ЕС) 2015/849.

## Съдържание

|    |                                                                                                            |    |
|----|------------------------------------------------------------------------------------------------------------|----|
| 1. | Обща информация и обхват .....                                                                             | 3  |
| 2. | Оценка и управление на рисковете при дистанционно установяване на отношения с клиенти .....                | 4  |
| 3. | Методи за дистанционно установяване на делови взаимоотношения .....                                        | 7  |
| 4. | Контролни мерки и механизми за дистанционна електронна идентификация .....                                 | 8  |
| 5. | Допълнителни мерки за смекчаване на риска .....                                                            | 9  |
| 6. | Прекратяване на процеса по дистанционно установяване на делово взаимоотношение с клиент .....              | 10 |
| 7. | Вътрешна организация и обучение на персонала при дистанционно установяване на делови взаимоотношения ..... | 10 |
| 8. | Възлагане на дейности по дистанционната електронна идентификация на външни изпълнители .....               | 11 |
| 9. | Съхраняване на информация и защита на личните данни .....                                                  | 12 |

## 1. **Обща информация и обхват**

През последните години, особено след ограниченията в резултат пандемията от COVID 19 и последствията от нея, се наблюдава увеличаване в търсенето на решения за дистанционно установяване на делови взаимоотношения с клиенти, както в международен мащаб, така и в българския банков сектор. По тази причина е от съществено значение банките да разполагат с надеждни и ефективни средства за изпълнение на мерките за комплексната проверка на клиентите в този контекст.

Дистанционното установяване на делови взаимоотношения с клиенти се разглежда от:

- FATF - международния стандарт<sup>1</sup> (комплексна проверка и нови технологии),
- Директива 2015/849 на ЕС (в п.19 от преамбюла /нови технологии/; чл.13, пар.1, букви а), б), в) – комплексна проверка, чл.25-29 – при възлагане на определени функции на трети лица от банките и чл. 8, пар. 3 и 4, буква а) политики, процедури и механизми за контрол, когато мерките за комплексна проверка на клиенти се извършват дистанционно) и
- Насоки на ЕБО<sup>2</sup> EBA/GL/2022/15 (относно използването на решения за дистанционно установяване на делови взаимоотношения с клиенти), които се прилагат от 02.10.2023 г. за банките, съгласно решение на УС на БНБ № 231/18.05.2023 г.

Насоките EBA/GL/2022/15 допълват следните 5 предходно издадени от ЕБО насоки относно:

- Насоки съгласно член 17 и член 18, параграф 4 от Директива (ЕС) 2015/849 относно комплексната проверка на клиента и факторите, които кредитните и финансовите институции следва да вземат предвид при оценката на риска от изпиране на пари и финансиране на тероризма, свързан с индивидуални делови взаимоотношения и случайни сделки („Насоки относно рисковите фактори, свързани с ИП/ФТ“), за отмяна и замяна на Насоки JC/2017/37, (EBA/GL/2021/02);
- Насоки относно вътрешното управление съгласно Директива 2013/36/ЕС (EBA/GL/2021/05);
- Насоки относно политиките и процедурите, свързани с управление на нормативното съответствие, и ролята и отговорностите на служителя, отговорен за нормативното съответствие във връзка с БИП/БФТ, съгласно член 8 и глава VI от Директива (ЕС) 2015/849 (EBA/GL/2022/05)
- Насоки за възлагане на дейности на външни изпълнители (EBA/GL/2019/02);
- Насоки относно управление на риска в областта на ИКТ и сигурността (EBA/GL/2019/04).

---

<sup>1</sup> Понастоящем това са препоръки 10 и 15 от 40<sup>те</sup> препоръки на FATF, 2012 г. (предходни 5 и 8), чиито последващи ревизии не касаят комплексната проверка и новите технологии, с изключение на виртуалните активи и доставчиците на виртуалните активи.

<sup>2</sup> Съгласно чл. 16 от Регламент 1093/2010 (за създаване на Европейския банков орган)

## **2. Оценка и управление на рисковете при дистанционно установяване на отношения с клиенти**

При дистанционно установяване на делови взаимоотношения с клиенти (без присъствието на клиента<sup>3</sup>) банките трябва да разполагат с дистанционен електронен процес и технологично решение, които са подходящи за валидиране и проверка на идентичността на физическите лица, въз основа на документи, данни и информация от надежден и независим източник.

Идентифицирането на клиента и проверката на идентификационните данни може да се извършват чрез средства за електронна идентификация, съответни удостоверителни услуги, предвидени в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар или по друг признат с нормативен акт начин за електронна идентификация или квалифицирана удостоверителна услуга по смисъла на същия регламент.

Банките, като задължени лица по ЗМИП, трябва задълбочено да оценят рисковете, произтичащи от дистанционната електронна идентификация на физически лица, по отношение на самите физически лица, надеждността и независимостта на източниците, използвани за проверка на самоличността, продуктите или услугите, които ще се предоставят на клиентите, както и географските и други рискови фактори. Въз основа на горепосочената оценка на риска, банките следва да установят процес и технологично решение за дистанционна електронна идентификация по подходящ начин и в съответствие с приложимите регулации, ЗМИП (и др. релевантни закони) и да осигурят ефективното им прилагане.

Банките трябва внимателно да проверяват валидността и автентичността на данните, документацията и информацията, получени по отношение на физическите лица, част от процеса на дистанционна електронна идентификация, като използват подходящ набор от данни от различни, надеждни и независими източници и като имат предвид, че данните, получени по електронен път от документ за самоличност на физическо лице, което не присъства физически, не са достатъчни за удостоверяване на самоличността му, освен ако не са придружени от необходимите мерки и механизми за контрол, предвидени в ЗМИП и ППЗМИП.

Преди да приемат процес на дистанционна електронна идентификация и приложат съответното технологично решение, банките извършват информирана оценка за:

- възможността избраното технологично решение:
  - да бъде напълно интегрирано в техните съществуващи системи и процеси,
  - дали съществуват технически и оперативни рискове, технологичното решение да бъде: ненадеждно, подправено или да претърпи непоправима повреда.
- рисковете, свързани с качеството, по-специално рискът източниците на информация, използвани за целите на проверката, да не са достатъчно независими и надеждни, както и рискът степента на проверка на самоличността, осигурена от технологичното решение, да не съответства на нивото на риска от изпиране на пари и финансиране на тероризма, свързан с физическото лице;

---

<sup>3</sup> ЗМИП (чл. 53, ал.7 във връзка с чл.55, ал.2 - един или повече от 8 способа за проверка) и ППЗМИП (съотв. чл. 41 и чл. 42, чл.44, ал.3 и чл.60, ал.3)

- рискове от измама с фалшива/подправена самоличност, т.е. риск, че дадено физическо лице не е това, за което се представя, или че лицето реално не съществува;
- риска, технологичното решение да не отговаря на приложимото законодателство за защита на личните данни.

По отношение на техническите и оперативните рискове банките, като задължени по ЗМИП лица, трябва да разполагат с достатъчен вътрешен (за конкретната банка) експертен опит, в допълнение към всички външни експертни съвети/консултантски решения/възлагане на дейности на външни изпълнители, за да гарантират правилното внедряване и използване на технологичното решение, както и да осигурят продължаването на услугите, ако технологичното решение претърпи непоправима системна повреда или в случай на прекратяване на бизнес отношенията между банката и външния доставчик на решението (когато то не е разработено вътрешно, в банката). За тази цел, следва да се предвиди въвеждане на подходящ план за действие при извънредни ситуации, който осигурява непрекъсваемост на услугата за дистанционно установяване на делови взаимоотношения с клиенти.

Преди внедряване на технологично решение за дистанционно установяване на делови взаимоотношения с клиент, банките трябва да проведат подходящи тестове, за да установят дали процесът на дистанционна електронна идентификация и технологичното решение са адекватни и надеждни<sup>4</sup> и позволяват прилагането на мерки за разкриване на информация в съответствие с политиките и процесите им в областта на борбата с изпирането на пари и финансирането на тероризма (БИП/БФТ) и приложимото национално законодателство в тази област. Служителят, отговарящ за нормативното съответствие във връзка с БИП/БФТ, следва да докладва резултатите от тази информирана оценка за рисковете при дистанционно установяване на делови взаимоотношения с клиенти на ръководния орган на банката, като внедряването на такова технологично решение не следва да започва, докато не бъдат налични и ефективно приложени подходящи ресурси за разбиране и управление на свързаните с него рискове.

Ръководството на банката следва да има задълбочено разбиране на рисковете от процеса на дистанционна електронна идентификация и приложеното технологично решение, като внедряването на процеса стартира след одобрението му от ръководството на банката.

Одобреният процес на дистанционна електронна идентификация трябва да включва най-малко:

- поэтапно описание на процеса на дистанционна електронна идентификация по метода, прилаган съгласно т. 3 от настоящия документ, и организационните, техническите и процедурните гаранции, които осигуряват надеждното идентифициране и валидиране на самоличността на физическите лица и управлението на съответните рискове, както и спазването на разпоредбите на ЗМИП, ЗЗЛД<sup>5</sup> и гореспоменатите насоки, издадени от ЕБО, за които УС на БНБ е взел решение за спазване;

---

<sup>4</sup> Тестовите следва да включват и проверка дали данните, които се съхраняват в технологичното решение, могат да се променят (фалшифицират) или подменят по някакъв начин и дали има регистър на действията, които се извършват в системата/технологичното решение (логове).

<sup>5</sup> Закон за защита на личните данни.

- процедури за включване на допълнителни мерки и гаранции, които се задействат, в случай на недостатъчна степен на сигурност по отношение на валидността на документа за самоличност или самоличността на физическото лице;
- процедура за регистриране и наблюдение на всички отклонения от одобрения процес на дистанционна електронна идентификация; и
- критерии за неприемлив риск и процедура за прекратяване на процеса на дистанционна електронна идентификация, когато тези критерии са изпълнени.

В зависимост от оценката на риска, банките следва да преразглеждат периодично процеса на дистанционна електронна идентификация и прилаганото технологично решение (напр. ежегодно), като отчитат технологичното развитие, възникващите рискове и всички промени в националната рамка за БИП/БФТ, за да се осигури вземането на информирано решение относно пригодността им и необходимостта от въвеждане на допълнителни мерки и механизми за контрол, включително анализ на постъпили сигнали/жалби за извършени измами (при наличие на такива).

Банките трябва да отстраняват без неоправдано забавяне всички грешки или слабости в процеса на дистанционна електронна идентификация и в технологичното решение, които могат да бъдат установени в хода на работния процес на технологичното решение или по време на редовен преглед, като предприемат и следните допълнителни действия:

- преглед на всички засегнати делови взаимоотношения, за да се прецени дали приложените мерки за комплексна проверка на клиента са в съответствие с политиките и процесите на банката;
- след като слабостите бъдат отстранени и бъде приложена адекватна защита на данните, се извършва оценка дали засегнатите делови взаимоотношения могат да бъдат запазени, като се включат допълнителни мерки за комплексна проверка; следва да бъде прекратено извършването на определени сделки или да бъдат прекратени деловите взаимоотношения;
- оценка на това дали в резултат на горепосочените действия следва да бъде представена информация до органите за контрол по ЗМИП за установени проблеми и предприетите действия;
- необходимост от задълбочена допълнителна оценка за надеждността на технологичното решение, при установени слабости или системни грешки спрямо рисковете от ИП/ФТ, разглеждане на възможни подобрения за технологичното решение и оценка за продължаване/прекратяване използването на това технологично решение;
- Специализираната служба за Вътрешен одит на банките, при изпълнение на вътрешната одитна функция, отчитайки риска от дистанционното установяване на делови взаимоотношения, също трябва да включва специфичен одитен преглед за адекватност и надеждност на технологичното решение, за осъществяване на дистанционно установяване на делови взаимоотношения с клиенти, като за резултатите от тези проверки се информира и служителят, отговорен за нормативното съответствие във връзка с БИП/БФТ, в контекста на мониторинг и оценка на прилаганите ИП/ФТ политики и процедури;

- Възможност за извършване на независим одит на процеса по дистанционна електронна идентификация, включително технологичното решение.

### 3. Методи за дистанционно установяване на делови взаимоотношения

Банките, като задължени по ЗМИП лица, са внедрили различни технически решения за дистанционно установяване на делови взаимоотношения с клиенти:

- присъствени решения (с участието на служител на банката) за дистанционно установяване на делови взаимоотношения с клиенти, при които клиентът взаимодейства със служител за извършване на процеса на проверка, например видеоконферентна връзка със служител на банката, преминал подходящо обучение по темите, свързани с превенция на ИП/ФТ, която се състои в интерактивна аудиовизуална връзка в реално време между физическото лице и служителят (участниците във видеовръзката се намират на различни локации, а връзката позволява непосредствен обмен на файлове и съобщения);
- неprisъствени решения (без участието на служител на банката) за дистанционно установяване на делови взаимоотношения с клиенти, при които клиентът не взаимодейства със служител за извършване на процеса на проверка – например автоматизирано решение за дистанционно установяване на делови взаимоотношения с клиенти в реално време, без човешка намеса, чрез снимки или видеоматериали, направени в момента, в който клиентът преминава процеса на проверка, вкл. запис на звук.

За целите на дистанционната електронна идентификация, са допустими оригинали на лични документи, описани в ЗМИП<sup>6</sup>, за които са налични данни в PRADO (Public Register of Authentic travel and identity Documents Online<sup>7</sup>) и които имат: снимка и подпис на притежателя; машинночитаема зона<sup>8</sup> (MRZ); две допълнителни усъвършенствани функции за визуална сигурност/защита сред посочените от PRADO<sup>9</sup>. След преценка на риска, банките могат да приемат като документ за самоличност на български граждани лична карта, издадена от МВР, с пълно име, изписано и на латиница, без машинночитаема зона, при условие, че в рамките на процеса на видеоконферентния метод е включена и проверка на документа в онлайн регистъра на МВР - [Справка за валидност на български лични документи \(mvr.bg\)](#).

Когато банките използват неprisъствени решения за дистанционно установяване на делови взаимоотношения с клиенти, те прилагат допълнителните мерки за намаляване на риска от ИП/ФТ (т. 5 от настоящия документ).

<sup>6</sup> Лични документи - съгласно пар. 1, т. 12 от ДР на ЗМИП.

<sup>7</sup> Публичен онлайн регистър на ЕС за документи за самоличност и пътуване - [Council of the European Union - PRADO - Home \(europa.eu\)](#)

<sup>8</sup> Съгласно § 1, т. 11 от Допълнителните разпоредби на Закона за българските лични документи.

<sup>9</sup> В допълнение към посочения публичен регистър, банките могат да използват и други надеждни източници относно установяване на реквизитите на документите за самоличност.

#### 4. Контролни мерки и механизми за дистанционна електронна идентификация

Банките трябва да разполагат с контролни мерки и механизми за гарантиране на надеждността на процеса на дистанционна електронна идентификация, както следва:

- Да приемат усъвършенствани технически спецификации за проверка на автентичността, валидността и целостта на документите за самоличност, като се уверяват, че те не са били променяни или фалшифицирани по какъвто и да е начин (например чрез промяна/подмяна на данни от истински документ, създаване на фалшив документ за самоличност, като се използват материали от легитимни документи). За тази цел представените документи за самоличност се проверяват спрямо спецификациите на всеки документ, описани в PRADO, по-специално защитните елементи, вида и размера на знаците и структурата на документа. Освен това се проверява автентичността на документа за самоличност, от една страна, чрез разчитане и дешифриране на информацията, включена в MRZ, и от друга страна, чрез проверка на още поне два визуални защитни елемента от посочените в PRADO;
- Да гарантират надеждността на процеса на дистанционна електронна идентификация, като разчитат, доколкото е възможно, на множество алтернативни източници на информация. Надеждността на процеса на дистанционна електронна идентификация се повишава, когато банките черпят данни от [Справка за валидност на български лични документи \(mvr.bg\)](http://mvr.bg);
- Да извършват проверки за съответствие с профила на физическото лице, документа за самоличност и всякаква друга информация, като се използват данни от надеждни и независими източници;
- Да създадат възможност за динамичен процес на дистанционна електронна идентификация, като разработят алтернативни стандартни методи за идентификация и прилагат/избират на случаен принцип един от тях.

Банките приемат технически и предпазни мерки в процеса на дистанционна електронна идентификация, независимо от използвания метод, както следва:

- Прилагане на техники за сигурна комуникация между банката, като задължено лице по ЗМИП, и физическото лице, като гарантират целостта и поверителността на обменяната информация;
- Гарантиране на извършването в реално време и без прекъсвания на процеса на дистанционна електронна идентификация, като не се приемат файлове, свързани с идентификацията, създадени от физическото лице по какъвто и да е начин преди започването на процеса;
- Гарантиране недвусмислена разпознаваемост на физическото лице и неговия документ за самоличност (всички снимки и видеоклипове, направени по време на процеса на дистанционна електронна идентификация, да са с добро качество, налице да са подходящи условия на осветление, подходящо разстояние от камерата, незакриване на части от лицето или документа и необходимите данни да са заснети ясно и не са налице предпоставки за съмнение);

- Гарантиране на съхранението на цифров носител, надлежно защитен от опити за подправяне на всички получени данни, както и на резултатите от проверките, извършени на различните етапи от процеса на дистанционна електронна идентификация - всички снимки или видеозаписи, направени по време на процеса на дистанционна електронна идентификация;
- Гарантиране, че по време на целия процес на дистанционна електронна идентификация се използва само едно устройство.

Като част от процеса на дистанционна електронна идентификация и независимо от използвания метод, банките прилагат специфични мерки и контроли, например:

- Правене на снимки при подходящо осветление, на които ясно се вижда: лицето под различни ъгли, напр. в профил, в анфас, като успоредно с това се използват техники за осигуряване на разпознаване на движение (например отворени очи, затворени очи); и страните на документа за самоличност, върху които са поставени снимката, подписът и данните на физическото лице, за да могат да бъдат проверени спрямо спецификациите и защитните елементи на документа;
- Използване на надеждни алгоритми за биометрично сравнение на физическото лице със снимката в документа за самоличност;
- Изискване от физическото лице да въведе уникален номер, изпратен по електронна поща или чрез текстово съобщение до мобилен телефон;
- Използване на специализирано техническо средство за автентикация в реално време на данните от устройството на потребителя.

В контекста на метода за дистанционна електронна идентификация банките, в допълнение към горното, могат да:

- помолят физическото лице да постави пръст върху зоната за сигурност на документа за самоличност или да премести ръката си пред лицето си;
- в случай на лични карти, издадени от МВР, да провери също дали има признаци, че покритието на картата е повредено или подправено, има признаци за опит за фалшифициране на документа, или снимката е поставена в документа след издаването му;
- да установи подозрително поведение на физическото лице, което може да показва, че то е под влияние на опиати или е подложено на натиск от външни фактори, или е с психически отклонения.

## 5. Допълнителни мерки за смекчаване на риска

Когато банките прилагат процеса на дистанционна електронна идентификация, без физическото присъствие на банков служител, те трябва да предприемат и допълнителни мерки за намаляване на риска, (неизчерпателно изброени), например:

- да гарантират, че първият превод по сметката на физическото лице е направен от сметка, водена на негово име в кредитна или финансова институция от държава

членка на ЕС, или в държава членка на FATF. Банките могат алтернативно да потвърдят съществуването на горепосочената сметка, като получат информация от самата кредитна или финансова институция, както и от всеки друг надежден и независим източник;

- да се потвърди регистрация/нареждане на плащане или достъп до дистанционните канали (мобилно/онлайн банкиране) чрез въвеждане на генериран код (SMS потвърждение например);
- провеждане на телефонен разговор и потвърждение на лична информация преди извършване на операция/сделка с по-висок риск от ИП/ФТ;
- използване на информация, която може да се извлече от устройството на клиента, за да се потвърди определена лична информация (IP адрес, местоположение на мобилно устройство, за да се потвърди адрес).

## **6. Прекратяване на процеса по дистанционно установяване на делово взаимоотношение с клиент**

Банките следва да гарантират, че процесът на дистанционна електронна идентификация се прекратява, без да бъде завършен, в някой от следните случаи:

- визуалното удостоверяване на физическото лице или на официалния документ за самоличност не е възможно или е налице несъответствие;
- има несъответствие между данните и информацията, предоставени по време на процеса на дистанционна електронна идентификация, и данните, получени от друг надежден и независим източник;
- налични са съмнения за висок/неприемлив риск от изпиране на пари и финансиране на тероризъм.

Причината за прекратяване на процеса на дистанционна електронна идентификация се документира и съхранява в подходящо защитен запис за предвидения по закон период и/или в съответствие с политиката на банката за защита на личните данни.

## **7. Вътрешна организация и обучение на персонала при дистанционно установяване на делови взаимоотношения**

Банките гарантират, че процесът на дистанционна електронна идентификация се извършва от квалифициран и обучен персонал, на когото са предоставени необходимите ресурси и специални технически средства за безпроблемно и сигурно изпълнение на процеса. Обучението включва практическото прилагане на технологичното решение и неговите функционалности; познаване на защитните елементи на документите за самоличност; обичайните методи прилагани при подправяне и фалшифициране; изискванията на закона; идентифициране на необичайни или подозрителни трансакции и докладване в съответствие с вътрешните процедури.

Обучението следва да се провежда преди заемане на длъжността от служителите, ангажирани в процеса на дистанционно установяване на отношения, и регулярно като

допълнение към общото обучение за БИП/БФТ, съгласно приложимата ИП/ФТ рамка на съответната банка.

Банките следва да гарантират чрез подходящи процедури, че персоналът, ангажиран с идентифицирането и валидирането на идентичността на клиентите чрез технологичното решение за дистанционна идентификация, не си сътрудничи с лица, замесени в незаконни дейности. Тези процедури включват оценка на пригодността на служителите за изпълнение на служебните задължения:

- преди наемане на работа; и
- регулярно по време на работния процес;
- случайно разпределение на заявленията на физическите лица за дистанционна електронна идентификация между служителите, така че да се сведе до минимум рискът от манипулиране; и
- проверки на извадков принцип от комуникацията на служителите с физически лица по време на или след процеса на дистанционна електронна идентификация.

В процеса на дистанционно установяване на делови взаимоотношения, банките гарантират, че ангажираните служители се намират в специално проектирана зона с ограничен достъп.

## **8. Възлагане на дейности по дистанционната електронна идентификация на външни изпълнители**

Ако банките решат да възложат, изцяло или частично, процеса на дистанционна електронна идентификация, те трябва да гарантират чрез подходящи процедури за оценка и контрол, че външният доставчик на услуги е приел технически спецификации и предпазни мерки, гарантиращи надеждна идентификация и валидиране на идентичността на физическите лица, в съответствие с процеса на дистанционна електронна идентификация на банката. Във всеки случай крайната отговорност за спазването на разпоредбите на ЗМИП и изискванията на рамката за превенция ИП/ФТ се носи от възлагащата страна (конкретната банка). Тази отговорност включва непрекъснат мониторинг на ефикасността и надеждността на процеса на дистанционна електронна идентификация и предоставяне на изрично предварително одобрение на всяка модификация на процеса от външния доставчик на услуги.<sup>10</sup>

Банките гарантират, че външният доставчик на услуги е обвързан с договорни отношения за изпълнение на задълженията си по споразумението за възлагане на външни услуги в съответствие с разпоредбите на ЗМИП и приложимата институционална рамка за конкретната банка. В споразумението за възлагане на външни услуги се определят ясно и подробно ролите, отговорностите, правата и задълженията на всяка от страните, включително тези, които произтичат от изтичането на срока на споразумението или от предсрочното му прекратяване, като в този случай се задейства план за излизане, включително прехвърлянето на всякаква информация и данни, получени от външния доставчик на услуги при изпълнението на споразумението. В споразумението за възлагане на външни услуги изрично се предвижда, че не е възможна промяна в процеса на дистанционна електронна идентификация без предварителното одобрение на банката, както

---

<sup>10</sup> Прилагат се Насоки за възлагане на дейности на външни изпълнители (EBA/GL/2019/02).

и че банката във всеки един момент има достъп до данните, документацията и информацията, които са събрани от външния изпълнител.

Банките гарантират, че външният доставчик на услуги:

- предоставя адекватна и точна информация за използваните източници, извършените проверки и резултатите от процеса на дистанционна електронна идентификация за всяко физическо лице, което позволява на банката да оцени качеството на процеса и да установи надеждността на идентификацията и проверката;
- е в съответствие със законодателството за защита на личните данни и е сертифициран за прилагане на стандарти за информационна сигурност;
- е въвел обучение, което включва практическото прилагане на технологичното решение и неговите функционалности; познаване на защитните елементи на документите за самоличност; обичайните методи за подправяне и фалшифициране; изискванията на законодателството; идентифициране на необичайни или подозрителни трансакции и докладване в съответствие с вътрешните процедури.

Когато външният доставчик на услуги се намира в друга държава (извън Република България), банките следва да предвидят свързаните с това правни и оперативни рискове и с изискванията за защита на личните данни. Банките не наемат външни доставчици на услуги, намиращи се в друга държава, в която са въведени правни ограничения, които не позволяват свободния обмен на информация между външния доставчик на услуги и задълженото лице или БНБ, или спазването от страна на външния доставчик на услуги на рамката за противодействие на изпирането на пари/финансирането на тероризма.

Цялостното или частично изпълнение на процеса на дистанционна електронна идентификация от външен доставчик на услуги и връзката на последния с конкретна банка в никакъв случай не трябва да застрашава функционирането и качеството на системата за вътрешен контрол на банката, както и възможността на БНБ да проверява по време и начин, които счита за целесъобразен и подходящ, спазването на задълженията на банката, произтичащи от разпоредбите на ЗМИП и др. подзаконовни актове.

## **9. Съхраняване на информация и защита на личните данни**

Банките спазват изискванията ЗМИП за съхраняване на архив, както и законодателството за защита на личните данни, независимо от вида или външния доставчик на технологичното решение, което използват в дистанционния процес на електронна идентификация.

Банките трябва да съхраняват непокътнати (в оригинал/без допълнителна намеса) всички необходими записи/данни получени по време на процеса на дистанционна електронна идентификация. Банките гарантират, че физическите лица са информирани за обработването на техните лични данни. По отношение на биометричната и дистанционната електронна идентификация се изисква изричното и конкретно съгласие на физическите лица.