

## **УКАЗАНИЯ ЗА ИЗГРАЖДАНЕ НА СИСТЕМИ ЗА ПРЕВЕНЦИЯ СРЕЩУ РИСКА ОТ ИЗПИРАНЕ НА ПАРИ**

Настоящите указания се издават от БНБ на основание чл. 73, ал. 3, във връзка с ал. 1, т. 8 от Закона за кредитните институции и са съгласувани с ДАНС. С тях се определят основните насоки, които банките следват при изграждането на системите за превенция срещу риска от изпирането на пари. Прилагането от всички банки на унифициран подход при анализ на риска е условие за изграждане на ефективни системи за наблюдение, контрол и предотвратяване на опити за умишлено или неволно използване на банковия сектор за изпиране на пари и финансиране на терористични действия или на опити за злоупотреби с банковите продукти и услуги.

Указанията са съобразени с документа „Общо съгласие за задълженията, произтичащи от европейския Регламент 1781/2006 относно информацията за платеца, съпътстваща паричните преводи, към доставчиците на платежни услуги на получателя”, приет през 2008 г. от трите комитета- Комитета на европейските банкови надзорници, Комитета на европейските надзорници по застраховане и доброволно осигуряване и Комитет на европейските регулаторни органи за ценни книжа с цел надзорен принос по въпросите на борбата с изпирането на пари и финансирането на тероризма с конкретен фокус върху Трета директива срещу изпирането на пари.

През последните години изпирането на пари се превърна в глобален проблем. Международният характер на търговията, системите за разплащане, навлизането на нови технологии, дават възможност за успешно (в някои случаи) прикриване и трансфериране на големи потоци мръсни пари чрез тяхното смесване със средства, придобити от легален бизнес. Затова са необходими съвместни усилия на държавите членки на Европейския съюз, членовете на FATF, MONEYVAL и останалите регионални структури, за да се координират действията и засили превенцията. Изграждането на унифицирана законодателна рамка е първата и важна стъпка в превенцията. Ефективното ѝ прилагане е другото важно условие за успешни действия.

Указанията са структурирани в четири части:

1. Риск от изпиране на пари и финансиране на тероризъм
2. Анализ на риска от изпиране на пари и финансиране на тероризма при извършване на операции или установяване на отношения с клиенти
3. Управление на риска от изпиране на пари и финансиране на тероризма
4. Професионално обучение на банковите служители, отговорни за прилагането на мерки срещу изпирането на пари и финансирането на тероризма.

### **1. Риск от изпиране на пари и финансиране на тероризъм**

Рискът от изпиране на пари и финансиране на тероризъм се изразява във вероятността клиентът да използва финансовата система за изпиране на пари или финансиране на терористични дейности и/или лица, което от своя страна би застрашило икономическата стабилност на банките или доверието във финансовия сектор като

цяло. От банките се очаква в рамките на функционирането на системите за контрол да съблюдават широк спектър от възможни рискове от изпиране на пари, финансиране на тероризъм, измами, злоупотреба с вътрешна информация.

Изпиране на пари по смисъла на ЗМИП е:

1. преобразуването или прехвърлянето на имущество, придобито от престъпна дейност или от акт на участие в такава дейност, за да бъде укрит или прикрит незаконният произход на имуществото или за да се подпомогне лице, което участва в извършването на такова действие с цел да избегне правните последици от своето деяние;
2. укриването или прикриването на естеството, източника, местонахождението, разположението, движението или правата по отношение на имущество, придобито от престъпна дейност или от акт на участие в такава дейност;
3. придобиването, владението, държането или използването на имущество със знание към момента на получаването, че е придобито от престъпна дейност или от акт на участие в такава дейност;
4. участието в което и да е от действията по т. 1–3, сдружаването с цел извършване на такова действие, опитът за извършване на такова действие, както и подпомагането, подбуждането, улесняване извършването на такова действие или неговото прикриване.

Изпиране на пари е налице и когато дейността, от която е придобито имуществото по т. 1, е извършена в друга държава и не попада под юрисдикцията на Република България.

"Финансиране на тероризъм" по смисъла на българското законодателство е прякото или косвеното, незаконното и умишленото предоставяне и/или събиране на парични средства, финансови активи или друго имущество и/или предоставяне на финансови услуги с намерение те да бъдат използвани или със съзнанието, че ще бъдат използвани, изцяло или частично, за извършване на тероризъм по смисъла на Наказателния кодекс.

Изпирането на пари и финансирането на тероризъм могат да причинят негативни последици за финансовата система и за репутацията на страната. Поради това законодателството на България инкриминира тези деяния.

## **2. Анализ на риска от изпиране на пари и финансирането на тероризъм**

Всяка банка разработва и приема система за контрол и предотвратяване изпирането на пари и финансирането на тероризъм при работа с клиенти. Част от системата включва прилагане на адекватни процедури за установяване на бизнес отношения с клиенти, като например за изпълнение на операции на стойности над определените в закона прагове или за извършване на повече от една операция от клиент, които поотделно не надвишават определените прагове, но са налице данни, че операциите са свързани.

За целите на настоящите указания, клиентът се определя като:

- физическо или юридическо лице, което има открита банкова сметка или е установило бизнес отношения с банката;
- лице, в чиято полза е открита банкова сметка (действителният собственик);
- клиент на лице по чл. 3, ал. 2, т. 11 и 28 от ЗМИП, открило банкова сметка за депозиране на суми на цитирания клиент;

- физическо или юридическо лице, което няма открита сметка в банката и не е установило бизнес отношения с нея, но което изпълнява чрез банката операция/и на стойности над определените в закона прагове или извършва повече от една операция, която поотделно не надвишава определените прагове, но са налице данни, че операциите са свързани.

При ежедневната дейност на банката се създава възможност за събиране на достатъчно информация за самоличността на клиентите и за характера на техния бизнес, което от своя страна позволява на банката да управлява по-добре рисковете, свързани с установените отношения. Анализът на информацията и преценката за изискване на допълнителни данни се извършват като се следват процедури за прилагане на подход, базиран на риска. Процедурите отчитат влиянието на различните критерии, а именно тип клиент, географско разположение, продукти и услуги. Всеки от критериите има съществено значение при определяне на рисковия профил на клиента.

Процедурите, определящи рисковото базирано поведение, следва като минимум да уреждат:

- 2.1 начин на установяване качеството на клиента да принадлежи към групата лица, с които банката може да установява бизнес отношения (съобразно политика за одобрение на клиент);
- 2.2 начин за идентифициране и проверка на идентификационните данни за клиента;
- 2.3 оценка на рисковия профил на клиента;
- 2.4 мониторинг и анализ на операциите и сделките на клиента.

## **2.1 Политика за одобрение на клиент**

Препоръчва се всяка банка да приеме своя политика за одобрение на клиентите си. Политиката включва определени критерии и параметри, според които се преценява дали да се установят бъдещи отношения с потенциалния клиент на банката.

Приетата и прилагана от банката политика за одобрение на клиентите не трябва да е твърде рестриктивна и не трябва да води до отказ от предлагане на определени дейности на публиката, включително на лица с нисък финансов и социален статус.

Определят се граници на допустимия риск по отношение на: характер на бизнеса на клиента; място на регистрация или основно място на търговска дейност за юридическо лице; адрес на постоянно пребиваване, гражданство за физическо лице; начин и форма на извършване на паричните преводи; годишен/месечен обем на трансакциите; социално положение и финансово състояние.

Информацията, която се събира от клиента при установяване на делови отношения и при откриване на банкова сметка е поверителна и следователно не се разкрива или разгласява, освен в случаите, определени със закон. Със същия статут се ползва и информацията, която постъпва в банката в периода до прекратяване на деловите отношения. Нейният обем и съдържание кореспондират със степента на риска, свързан със съответния клиент.

Допълнителна информация, в рамките на нормативно определената, може да се изиска от клиента след откриване на сметката или по време на установяване на отношението при наличие на условията по чл. 1 , ал.ал. 3 и 5 от ППЗМИП.

Събирането на информация и осигуряването на нейния трансфер заедно с извършваните презгранични преводи се осъществява съгласно изискванията на Регламент (ЕО) № 1781/2006 на Европейския парламент и на Съвета, и на националното законодателство.

## 2.2 Начин за идентифициране на клиента и проверка на неговите идентификационни данни

Преди установяване на делови отношения с клиент, банката се задължава да го идентифицира и провери идентификационните данни. Процедурата включва установяване на самоличността на клиента въз основа на надеждни, независими и обективни източници. Извършването на проверка се удостоверява, като върху хартиения носител, съхраняван в клиентското досие, се постави дата, час и име на лицето, което проверява информацията в регистъра. При поддържане на електронно досие, информационната система на банката следва да е организирана така, че да позволява последваща проверка за времето и служителя, извършил верификацията. При съмнение за верността на данните, банковият служител изисква писмено изявление от клиента или негов упълномощен представител, с което се удостоверява качеството на информацията. Изявлението се предоставя преди установяване на делови взаимоотношения или извършване на транзакция.

### 2.2.1 Установяване и проверка на идентичността на клиент - физическо лице

Банката установява и проверява самоличността на клиента, който е физическо лице, на неговия законен представител, или който е едноличен търговец, като проверява описаните по-долу документи. Събраните данни се съхраняват в клиентското досие и в информационната система на банката и като минимум следва да съдържат информацията съгласно Таблица No1:

**Таблица No 1 – Необходими данни за проверка идентичността на ФЛ**

Тип на клиента	Минимално необходими данни за проверка на идентичността
Физическо лице	<ul style="list-style-type: none"> <li>- име;</li> <li>- постоянен адрес и адрес за кореспонденция;</li> <li>- дата и място на раждане;</li> <li>- ЕГН, ЕНЧ, друг уникален идентификационен номер, определян от чуждата държава;</li> <li>- вид, номер на документа за самоличност с неизтекла валидност, който съдържа и снимка на клиента;</li> <li>- гражданство;</li> <li>- телефон (факс и адрес на електронна поща – в случай, че разполага с такива)<sup>1</sup>;</li> <li>- професия<sup>1</sup>;</li> <li>- работодател<sup>1</sup>;</li> <li>- дата на установяване на бизнес отношенията;</li> <li>- целта и характера на отношението, което е установено или предстои да бъде установено.</li> </ul>
ЕТ	<ul style="list-style-type: none"> <li>- наименование на лицето и фирмата, под която ще се извършва дейността;</li> <li>- адрес по седалище и управление, и адрес за кореспонденция;</li> <li>- предмет на дейност (посочва се основната дейност, която може да е съвкупност от няколко дейности);</li> </ul>

<sup>1</sup> Данните се събират след преценка, че съществува повишен риск

	<ul style="list-style-type: none"> <li>- дата и място на раждане на собственика;</li> <li>- ЕИК на търговеца, ЕГН, ЕНЧ или друг уникален идентификационен номер на собственика, определян от чуждата държава;</li> <li>- вид, номер на документа за самоличност с неизтекла валидност, който съдържа и снимка на клиента;</li> <li>- гражданство;</li> <li>- телефон (факс и адрес на електронна поща – в случай, че разполага с такива)<sup>1</sup>;</li> <li>- дата на установяване на бизнес отношенията, цел и характер на отношението, което е установено или предстои да бъде установено.</li> </ul>
Данни за упълномощеното лице	<ul style="list-style-type: none"> <li>- име на лицето;</li> <li>- постоянен адрес и адрес за кореспонденция;</li> <li>- дата и място на раждане;</li> <li>- ЕГН, ЕНЧ, друг уникален идентификационен номер, определян от чуждата държава;</li> <li>- Вид и номер на документа за самоличност с неизтекла валидност, който съдържа и снимка на клиента.</li> </ul>

Информация за характеристиките на документите за самоличност, издавани от държавите членки на ЕС и ЕИП може да се намери на интернет страницата:

<http://prado.consilium.europa.eu/>

## 2.2.2 Установяване и проверка на идентичността на клиент - юридическо лице

Банката проверява идентификационните данни на клиент-юридическо лице, като ги сверява с публикуваната информация в търговския или други подходящи публични регистри. Клиент - чуждестранно ЮЛ представя оригинал или нотариално заверено копие на сертификата за регистрация. Препоръчва се банката да не приема за разглеждане документи и техни копия, при които интервалът от време между датата на тяхното издаване/заверка и на тяхното представяне в банката е повече от 6 месеца.

Информацията, събирана от банката за клиент - юридическо лице, е представена в следващата таблица:

**Таблица No 2 – Необходими данни за проверка идентичността на ЮЛ**

Тип на клиента	Минимално необходими данни за проверка на идентичността
Юридическо лице	<ul style="list-style-type: none"> <li>- Наименование;</li> <li>- правно-организационна форма;</li> <li>- седалище, адрес на управление и адрес за кореспонденция;</li> <li>- предмет на дейност или цел, срок на съществуване;</li> <li>- органи на управление и представителство;</li> <li>- вид и състав на колективния орган на управление;</li> <li>- основно място на търговска дейност;</li> <li>- ЕИК;</li> <li>- идентификационен номер, ако лицето подлежи на вписване съгласно изискванията на ДОПК;</li> <li>- копие на лиценз, разрешение или регистрация за извършване на дейност (когато дейността подлежи на оторизационен режим);</li> <li>- оригинал или нотариално заверено копие на официално извлечение за актуално състояние и заверено копие от учредителен договор или акт;</li> <li>- телефон, факс и адрес на електронна поща;</li> <li>- дата на установяване на бизнес отношенията;</li> <li>- цел и характер на отношението, което е установено или</li> </ul>

	предстои да бъде установено.
Действителен собственик / Действителен собственик на фондация, организация с идеална цел или лице, осъществяващо доверително управление на имущество	<ul style="list-style-type: none"> <li>- име;</li> <li>- постоянен или настоящ адрес;</li> <li>- дата и място на раждане;</li> <li>- ЕГН, ЕНЧ, друг уникален идентификационен номер, определян от чуждата държава;</li> <li>- вид и номер на документа за самоличност с неизтекла валидност, който съдържа и снимка на клиента. Държава на издаване на документа;</li> <li>- възрастови граници на групата от физически лица, в чиято полза е създадено ЮЛ;</li> <li>- държава на адресна регистрация на лицата от групата;</li> <li>- професия на лицата от групата;</li> <li>- брой на лицата от групата.</li> </ul>
Данни за законния представител на ЮЛ	<ul style="list-style-type: none"> <li>- име на лицето;</li> <li>- постоянен или настоящ адрес;</li> <li>- дата и място на раждане;</li> <li>- ЕГН, ЕНЧ, друг уникален идентификационен номер, определян от чуждата държава;</li> <li>- вид и номер на документа за самоличност с неизтекла валидност, който съдържа и снимка на клиента. Държава на издаване на документа</li> </ul>

Проверка на идентификационните данни се извършва и при осъществяване на операция или сделка над 30 000 лева или тяхната равностойност в чужда валута, както и при извършване на операция или сключване на сделка в наличност на стойност над 10 000 лв. или тяхната равностойност в чужда валута. Когато нарежданията от страна на клиента се подават по електронен път, банката прилага специални процедури, изискващи от клиента въвеждане на цифров сертификат или други уникални идентификатори като например потребителско име, автентичен номер на транзакцията, парола, които да осигурят безспорно верифициране на клиента или неговия представител.

Банката може да изисква допълнителни документи и информация, която ще се събира от клиентите с различни нива на риск.

Банкова сметка не се открива или закрива (по искане на клиент) и отношения с клиент не се установяват, когато банката не е в състояние да приложи мерките за превенция, определени в чл. 3, ал. 1 от ЗМИП.

Банката не открива анонимни сметки или сметки на фиктивни лица.

Когато лице открива или оперира със сметка от името и за сметка на трето лице, то в банката следва да се представят достатъчно убедителни документи, доказващи пълномощията, изготвени съобразно националното законодателство на третото лице и удовлетворяващи в достатъчна степен изискванията на банката по отношение на характера и съдържанието на документа.

В политиката и правилата на банката се определя вида на проверките, които е необходимо да се направят преди установяване на ново отношение или откриване на нова банкова сметка, с цел предпазване от сключване на сделки с лица, с известно криминално минало или включени в списъците на лица, свързани с терористични дейности или терористични организации.

Правилата на всяка банка съдържат критерии за установяване на съмнителни трансакции, свързани с финансиране на терористични действия. Разработват се подходящи механизми за засилено наблюдение на сметки, за които се предполага, че са свързани с терористични организации. Своевременно се изпраща доклад до министъра на вътрешните работи, председателя на Държавна агенция „Национална сигурност” и САД „Финансово разузнаване” в случай, че предположението не отпадне.

Преди установяване на отношения с потенциални клиенти, задължително се проверява дали те не фигурират в списъците на лица и организации, свързани с терористична дейност, а при актуализация на тези списъци, се извършва регресна проверка за наличието на лица от клиентската база на банката в тези списъци. При съвпадение на потенциален клиент или клиент от базата данни с лице от списъците, незабавно се изпраща доклад до министъра на вътрешните работи, председателя на Държавна агенция „Национална сигурност” и САД „Финансово разузнаване”. Списък на държавите и организациите, спрямо които Република България прилага забрана или ограничения върху продажбата и доставките на въоръжение и на свързано с него оборудване, в съответствие с Резолуциите на Съвета за сигурност на ООН и решенията на Европейския съюз и на Организацията за сигурност и сътрудничество в Европа, е утвърден с Постановление на Министерски съвет и периодично се актуализира. Списък на лица и организации, спрямо които Европейският съюз е предприел санкционни действия, е публикуван на официалната страница на Европейския съюз на адрес:

[http://ec.europa.eu/external\\_relations/cfsp/sanctions/docs/measures\\_en.pdf](http://ec.europa.eu/external_relations/cfsp/sanctions/docs/measures_en.pdf)

### 2.2.3 Установяване на действителния собственик на юридическото лице

Установяването на действителния собственик съставлява част от процеса на идентификация на клиента и проверка на неговите данни.

Когато става дума за високо рискови клиенти, банката трябва да провери предоставените данни и да получи потвърждение от надежден и независим източник (например, ако единственият източник на данни за действителния собственик е писмена декларация, подписана от законния представител или пълномощника на клиента, преди да установи бизнес отношения, банката трябва да провери данните, до степен, че е уверена в структурата на собственост и управление на клиента). Банката може да получи информация за структурата на управление и собственост на базата на оригинален документ, издаден от службата към официалния търговски регистър на съответната страна, когато са налице законови задължения за вписване на тези обстоятелства. Допуска се представяне на нотариално заверено копие при невъзможност за представяне на оригинал.

За местно юридическо лице се препоръчва да се извършва пряка проверка в публичния търговски регистър, за да се съберат или да се потвърдят данните, свързани с действителния собственик на това юридическо лице.

За чуждестранно юридическо лице се извършва аналогична проверка в официалния регистър на съответната държава по седалище на регистрацията.

Независимо дали действителният собственик е местно или чуждестранно лице, за него се събира информацията, посочена в Таблица № 2 към т. 2.2.2.

Ако законният представител показва нежелание да предостави на банката необходимите данни за действителните собственици, делови отношения не следва да се установят. Препоръчително е ситуации, при които клиент (както и потенциален клиент) избягва представянето на всички необходими данни, да се разглеждат от

банката като индикатор за съмнителна дейност и да се прецени изпращане на доклад за съмнителна операции или сделка до САД „Финансово разузнаване”, ДАНС. Банката извършва преценка дали да установи (а в случай на вече установени, да продължи) делови отношения с клиента.

Редът за установяване на действителен собственик на клиент следва да съставлява част от пакета документи, формиращи вътрешните правила на банката за превенция срещу изпиране на пари и финансиране на тероризъм. В банката се събира документация за структурата на собственост и на управление на клиента. Задължително се установяват физическите лица, които пряко или непряко притежават повече от 25 на сто от дяловете или от капитала на клиент - юридическо лице, или на друга подобна структура, или пряко или непряко го контролират. Когато клиент е фондация, организация с нестопанска цел или друго лице, което осъществява доверително управление на имущество или разпределение на имущество в полза на трети лица, банката установява физическото лице, в полза на което се управляват или разпределят 25 на сто или повече от имуществото на клиента. В случай, че структурата на юридическото лице не позволява да се определят физическите лица – действителни собственици, то тогава се определя група от физически лица, в чийто основен интерес е създадена или действа фондация, организация с идеална цел или лице, осъществяващо доверително управление на имущество или разпределение на имущество в полза на трети лица. Банките могат да определят и по-строги изисквания съобразно тяхната практика.

При определяне на обхвата на изискваните документи и на задълбочеността на анализа на клиентския профил, банката се основава на резултатите от прилагането на рисковото базирано подход, с цел минимизиране на нейните разходи, които в крайна сметка се разпределят върху цената, заплащана от банковия клиент.

#### 2.2.4 Изисквания за идентификация и проверка на идентичността при по-особени случаи – насоки

##### 2.2.4.1 Сметки на доверители, тръст компании и компании с номинални собственици

В практиката има случаи, при които сметки на доверители, тръст компании и компании с номинални собственици се използват с цел заобикаляне на процедурите за идентификация. Банката следва да определи дали клиентът действа като номинален представител или довереник от името на трето лице. Събира се информация за характера на дейността на компанията. При откриване на сметка на името на тръст компания, банката следва да се увери в идентичността на довереника и на физическото лице, в чиято полза се управляват или разпределят 25 на сто или повече от имуществото. В случай, че физическото лице не може да бъде индивидуализирано, банката идентифицира групата физически лица, в чиято полза е създадено юридическото лице. Когато физическите лица, в чиято полза то е създадено, не фигурират в официалните документи за неговото учредяване и актуално състояние, се прилага способът, определен в чл. 6, ал. 2 от ЗМИП.

2.2.4.2 Банката трябва да е много внимателна по отношение на компании, които неофициално се ползват от трети лица за откриване на банкови сметки или за установяване на отношения, като умишлено се скрива от кредитната институция този факт. В случай, че банката установи подобен факт преди откриване на сметката или извършване на сделката, тя не встъпва в отношения с потенциалния клиент и не извършва сделката, като уведомява САД „Финансово разузнаване”. Когато банката установи горното впоследствие, след откриване на сметката или извършване на

сделката, тя извършва обстоен анализ на структурата на управление и контрол на юридическото лице, на произхода на средствата, с които оперира дружеството, и на лицата, които управляват дейността. Своевременно се изпраща доклад до САД „Финансово разузнаване“.

### 2.3 Оценка на рисковия профил на клиента

Както е описано в раздел 2.2, банката се задължава да извърши идентификация на клиента и провери идентификационните данни, като се снабди с определените в ЗМИП информация и документи. В допълнение се прилагат и останалите мерки, предвидени в закона, като например установяване на целите и характера на отношението с клиента, вида дейност, извършвана от него, произхода на средствата, с които предвижда да оперира през банковите си сметки. Събраната първоначална информация за клиента е основание за решение от страна на банката дали да установи отношения с него.

Информацията е и основа за изграждане на първоначалния рисков профил на клиента и за класифициране в съответна рискова категория. Рисковата класификация следва да се извърши от отдела в банката, разполагащ с най-много информация. Обичайно това е отделът, който пряко контактува с клиента при изпълнение на неговите операции и сделки. Освен класифицирането на нови клиенти чрез определяне на техния рисков профил, банката се задължава да извърши класификация и на съществуващите клиенти. Първоначалният рисков профил на клиента се основава на информацията, определена в ЗМИП и ППЗМИП, и освен идентификационните данни може да включва също и информация за социалното положение и финансовото състояние, характера и мястото на извършване на дейността, данни за неговите контрагенти. Видът и обхватът на мерките за превенция ще зависят от степента на установения риск. При изграждане на клиентския профил банката изисква такава информация, която е необходима за преценка на риска и не затруднява допълнително клиента с нейното предоставяне. Данните, съдържащи се в клиентския профил, съставляват банкова и търговска тайна и не се разкриват пред трети лица, освен в определените от закона случаи.

Банката класифицира своите клиенти в три основни групи, към които принадлежат съответно лица, носители на нисък, нормален или висок риск. Банката може да използва и допълнителни поднива към основните групи.

Докато е в бизнес отношения с клиента, банката периодично прилага мерките за комплексна проверка, за да поддържа актуални данни в клиентското досие и да проверява дали клиентът отговаря на критериите, съответстващи на определената му рискова група. Това означава например, че след като банката установи, че клиентският бизнес значително се различава от наличната информация в банката, то последната трябва допълнително да анализира новите дейности, извършвани от клиента и, при възможност, да установи причините за тази промяна. Цел на допълнителния анализ също е да се прецени необходимостта от промяна на рисковата категория.

Всяка банка разработва процедура за периодичен преглед на събраните данни за клиентите и за последваща оценка/преоценка на рисковия профил.

При определяне на рисковия профил се препоръчва прилагането на по-консервативния подход. Това означава, че ако даден клиент, на базата на целия набор от рискови фактори, попада в повече от една рискова група, окончателната класификация за клиента съответства на най-високата рискова група, определена за него.

При рисковата класификация на клиента банката отчита няколко основни фактора:

- вид на клиента – фактор Т
- географски регион (място на седалище, място на основна дейност, адресна регистрация на юридическото лице) – фактор Г
- вид използван банков продукт – фактор П

В следващите параграфи е описана процедурата за определяне на рисковия профил.

Класификацията на клиента в определена рискова категория е от изключителна важност за характера на бъдещите отношения и обхвата на прилаганите мерки за комплексна проверка от банката.

В зависимост от рисковата категория на клиента, банката прилага различни по обхват мерки, а именно:

- Разширени мерки за висок риск
- Нормални мерки за нормален риск
- Опростени мерки за нисък риск

### 2.3.1 Разширени мерки за комплексна проверка на клиент

Такива мерки се отнасят за следните групи лица:

- Отношения с банка-респондент от трета държава
- Отношения с политически изявено лице (PEP)
- Установяване на отношения без присъствие на клиента
- Други отношения

#### 2.3.1.1 Установяване на отношения с банка-респондент от трета държава

Отношенията, при които банка от трета държава желае да открие сметка в българска банка, са определени от ЗМИП като високорискови. При тяхното установяване се изисква прилагане на следните допълнителни мерки за комплексна проверка:

- събиране на достатъчно информация за респондентската институция, така че да се разбере напълно характера на дейността ѝ, нейната репутация и качеството на надзора;
- оценка на изградените в респондентската институция системи за контрол и превенция срещу изпирането на пари и финансирането на тероризъм;
- получаване на предварително одобрение на новите кореспондентски отношения от висшия мениджмънт на българската банка;
- документиране на съответните отговорности на всяка институция;
- изграждане на надеждна система за наблюдение, гарантираща че респондентската банка прилага мерките за комплексна проверка на клиентите, които имат пряк достъп до кореспондентската сметка, когато такъв достъп е договорен между двете банки. При поискване от страна на българската банка, респондентът предоставя данните, имащи отношение към комплексната проверка.

Банката преглежда информацията, представена от банката-респондент, извършва проверка, като я сравнява с публично достъпните или други официални източници, анализира наличните данни и преценява риска от установяване на отношения.

Препоръчва се, при установяване на такива кореспондентски отношения, да се изиска и мнението на ръководителя на специализираната служба за превенция срещу изпирането на пари и финансирането на тероризма.

Данните, които българската банка събира при установяване на кореспондентски отношения с банка от страна извън ЕС или извън страните от списъка по чл. 4, ал. 9 от ЗМИП, като минимум съдържат:

- дата на издаване и срок на валидност на лиценза за извършване на банкови услуги; институцията, издала лиценза и осъществяваща надзор върху дейността;
- описание на изпълнението на вътрешните процедури за предотвратяване на изпирането на пари и финансирането на тероризма, в т.ч. процедурите за проверка на клиентите, на реалните собственици, процедурите за докладване на съмнителни сделки и клиенти, за съхранение на документацията, други мерки, които банка прилага с цел превенция;
- описание на системата за превенция, прилагана от клонове, субсидиари и представителства на банката-респондент, базирани в трети страни;
- писмено изявление, че правната рамка на юрисдикцията, в която е базирана централата на банката, е адекватна на нормативните изисквания, приложими в рамките на ЕС;
- писмена декларация, че банката не оперира и няма да оперира като "шел-банка";
- писмена декларация, че банката не е установила и няма да установява отношения с "шел-банки".

ЗМИП забранява на банките да установяват кореспондентски отношения със „шел-банки”.

„Шел-банките” нямат право да извършват дейност на територията на Р България. Банката не установява кореспондентски отношения с банки извън България, които позволяват техните сметки да бъдат използвани от „шел-банки”. Банките трябва да бъдат изключително бдителни, когато продължават кореспондентските си отношения с банки-респонденти, базирани в страни със занижени стандарти за превенция срещу изпирането на пари и финансирането на тероризма.

### 2.3.1.2 Клиент, притежаващ качеството на политически изявено лице (PEP)

Процедурата за преценка дали едно лице може да се включи в списъка на видни политически личности се извършва по следните способы:

- Анализ на информацията, предоставена от клиента, и
- Извършване на проверка от страна на банката в публично достъпни регистри, за да установи, дали лицето фигурира в базата данни за PEP.

Неспазването на подходящи процедури и установяване на отношения с клиент, който попада в групата на PEP или чийто действителен собственик е PEP, без да е

идентифициран като такъв от банката, може да доведе до значителен правен и репутационен риск. Прилаганият от банката процес за комплексна проверка трябва да е ефективен, за да се установи своевременно качеството на клиента и да не съществуват притеснения по отношение на произхода на средствата, с които той ще оперира. В тази връзка се препоръчва използването на въпросници, проверка в официални или специализирани бази данни, проверка в общата публично достъпна информация.

С помощта на закупени от външни доставчици или разработени от банката програмни продукти се извършва както първоначална, така и текуща проверка на клиентската база, за да се установят настъпилите промени в статуса на клиентите. Всяка банка определя честотата на текущата проверка, като обичайната практика е тя да се извършва поне веднъж месечно. Процесът ще гарантира установяване на лица, чийто статус е променен след първоначалните делови отношения с банката или съответно след последната проверка в клиентската базата данни. В случай, че в резултат на проверката се установи лице с променен статус, поставящ го в категорията на PEP, за продължаване на отношенията се изисква одобрение от служител на ръководна длъжност, определен от мениджмънта на банката. Впоследствие клиентът се категоризира като PEP и спрямо него банката започва да прилага засилени мерки за комплексна проверка. За да установи дали един клиент заема или е заемал висша държавна длъжност, или е свързано с него лице, банката извършва следните действия:

- клиентът/потенциалният клиент попълва въпросник-декларация. Примерен образец е приложен към настоящите указания (Приложение №1);
- събира информация от публични източници;
- събира информация от специализирани продукти, поддържащи база данни за PEP.

Спрямо клиент – PEP банката прилага мерки, които са допълнителни към обичайните мерки, прилагани спрямо клиентите с нормален риск и включват:

- получаване на писмено одобрение от служител на ръководна длъжност, определен от мениджмънта на банката, когато за първи път се установяват отношения или за първи път/по време на бизнес отношенията се установи, че клиентът е придобил статус на PEP;
- предприемане на подходящи действия за установяване произхода на средствата, използвани в бизнес отношенията между банката и клиента. Задължението възниква и при извършване на отделна операция или сделка, без установяване на трайни търговски отношения с клиент или действителен собственик на клиент - юридическо лице, за когото е установено, че е PEP, независимо от стойността на операцията или сделката;
- спрямо PEP банката поддържа текущо разширено наблюдение върху търговските отношения.

В допълнение към изброените мерки могат да се приложат една или повече от разширените мерки за комплексна проверка, посочени в чл. 8, ал. 3 от ППЗМИП, като банката извършва преценка на вида и степента на тяхната достатъчност.

Всяка банка включва като част от системите си за управление на риска осигуряване на списък на лица-PEP, който трябва да е на разположение на служителите, пряко работещи с клиенти, а по преценка, до списъка могат да имат достъп и служители от други отдели (напр. кредитиране, изпълнение на валутни преводи).

## Процедура на прекатегоризиране на лице с прекратен статус на РЕР

Всяка банка включва във вътрешните си правила процедура за промяна в обхвата на прилаганите разширени мерки за комплексна проверка, когато се установи, че определено лице не може вече да се счита за РЕР. Процедурата трябва да се съобрази със законовото изискване за прилагане на разширените мерки за период от минимум една година, след като лицето е престанало да заема висша държавна длъжност.

### 2.3.1.3 Прилагане на мерките за комплексна проверка при установяване на бизнес отношения без присъствие на клиента

С въвеждането на интернет банкиране, все по-голям брой сметки се откриват от банките, без да се изисква физическо присъствие на бъдещия клиент в офис на банката. Тези случаи крият по-висок риск, поради което банката трябва да прилага подходящи мерки за неговото минимизиране. За да се увери в истинността на идентификационните данни, банката може да изиска всеки представен документ да бъде нотариално заверен за вярност на съдържанието или да й бъдат представени допълнителни документи. Допълнителен способ за управление на риска е въвеждане на изискване първото плащане по операция или сделка да се осъществи чрез сметка, открита на името на клиента в българска банка, клон на чужда банка, получила лиценз от Българската народна банка да осъществява дейност в страната чрез клон, или в банка от страна - членка на Европейския съюз.

Банката може да се възползва от възможността, предоставена в чл. 6а от ЗМИП и да се позове на данни от предходно идентифициране при наличие на условията, посочени в цитираната разпоредба.

Когато банка изнася дейността по идентификация на клиентите се следват „Указанията за изнасяне на дейности”, издадени от БНБ и съобразени със съответния документ на Комитета на Европейските банкови надзорници (КЕБН).

### 2.3.1.4 Други случаи

Освен посочените по-горе случаи, банка може да категоризира свои клиенти като носители на по-висок риск от средно допустимия, базирайки се на миналото на клиента, източника на средства, характера на неговите контрагенти, клиенти със съмнителна репутация в публичното пространство.

Примери, които могат да затруднят банката при определяне на произхода на средствата, са случаи, при които клиентът-юридическо лице има неясна или комплексна структура: тръстове; благотворителни организации; неправителствени организации; организации, получаващи дарение; компании с номинални собственици.

Банките прилагат разширени мерки за превенция при оценка за повишен риск.

### 2.3.2 Опростени мерки за комплексна проверка на клиент

В своята практика банките трябва да прилагат пълния набор от мерки за комплексна проверка, определени в чл. 3, ал.1 от ЗМИП. Международните стандарти и българското законодателство отчитат наличието на случаи, в които съществува минимален риск за

изпиране на пари и финансиране на тероризъм. В тези ситуации се допуска намаляване на обхвата на мерките при запазване на техния вид, освен ако не възникне съмнение за изпиране на пари или финансиране на тероризъм. Въпреки това следва да се подчертае, че опростеният режим не освобождава банките от всички задължения за добросъвестна проверка. Задължително е във всички случаи да се събира достатъчно информация за оценяване, дали клиентът или ползваният от него продукт отговарят на изискванията за ниско рисков случай.

Международните стандарти и Директива 2005/60/ЕО препоръчват да се осигури наличието на следните условия:

- достатъчна информация, въз основа на която да се прецени, дали конкретният клиент, продукт или сделка притежава характеристиките за прилагане на опростена комплексна проверка;
- съществуване на възможност за преценка на аномалии в клиентския профил. За целта банката следва да разполага с адекватна обективна и субективна информация и да извършва текущо наблюдение;
- банката да бъде в състояние да изпълнява задълженията си за съхраняване на информацията за клиента, по начин и в срок, определен от закона, така че при отправени запитвания от компетентните органи, да може да осигури данни за установените бизнес отношения с клиент.

Независимо от това, че клиент е категоризиран като ниско рисков и спрямо него се прилагат опростени мерки, то за банката остава задължението, при възникване на съмнение, че сделката или операцията е свързана с изпиране на пари, да разшири обхвата на мерките. С други думи, банката трябва:

- да познава клиентската самоличност, за да я посочи при изпращането на доклад за съмнителен случай;
- да наблюдава клиентските сделки, за да може да забележи съмнителни дейности.

В ЗМИП са предвидени минимума от мерки, които се прилагат към носителите на нисък риск. Възприетият подход отразява Европейската практика и се състои в следните стъпки:

- извършва се задължителна идентификация, която включва като минимум установяване на самоличността на клиента и проверка на представените данни;
- провежда се минимален мониторинг.

Примери за нисък риск са случаи, при които информацията за идентичността на клиента и действителния собственик на клиента е публично достъпна и известна, или където на национално ниво са разработени и се прилагат адекватни системи за проверка и контрол. При наличието на тези условия държавите-членки на Европейския съюз могат да разрешат на банките и финансовите си институции да прилагат опростени мерки при идентификацията и верификацията на данните за клиентите и действителните им собственици, както и при прилагане на останалите мерки.

Директива 2005/60/ЕО на Европейския парламент и на Съвета, както и Директива 2006/70/ЕО на Комисията са Европейски документи с минимум хармонизация. В тази връзка, националното законодателство може да предвиди по-рестриктивни от посочените в директивите мерки за превенция срещу изпирането на пари. Р България се е възползвала от дерогацията по отношение на лицата - носители на нисък риск за изпиране на пари, като за целта е определила, че опростени мерки могат да се прилагат единствено спрямо лицата, дефинирани в чл. 4, ал. ал. 9, 17, 18 и 19 ЗМИП.

Директива 2005/60/ЕО дава възможност на държавите – членки да разширят обхвата на лицата – носители на нисък риск за изпиране на пари, спрямо които се прилагат опростени мерки. Р България не се е възползвала от тази възможност, като в случая българският законодател, с оглед на местните условия, е приложил консервативен подход при транспониране на цитираните директиви в националното законодателство.

### 2.3.3 Рискови фактори, въз основа на които се определя нивото на риска за клиента

Международно приетите стандарти, на които се основава рисковото базирания подход, включват следните рискови фактори:

- тип на клиента: рисковият фактор е свързан със статута на клиента или с неговата дейност (например държавна институция, видни политически лица, лица, чиято дейност предполага опериране с големи обеми пари в брой, неправителствени организации и други подобни);
- държави, юрисдикции и географски райони, с които клиентът има взаимоотношения, адресна регистрация, регистрация по седалище; пример за висок риск, свързан с изпиране на пари или финансиране на тероризъм представляват държави или географски региони, за които е установено, че не прилагат в достатъчна степен международните стандарти за превенция, държавит с високо ниво на корупция или престъпна дейност, държави, на които са наложени публично обявени ограничителни мерки от международни организации.
- вид на ползвания продукт или услуга: всеки продукт или услуга, предлагани от банката, следва да се анализират дали крият рискове за изпиране на пари или финансиране на тероризъм. В обхвата на анализа попада всеки нов или иновативен продукт. Примери за продукт или услуга, които могат да съставляват висок риск са:
  - частно банкиране – обичайно това са услуги, предлагани на клиенти, чийто активи, депозирани в банката, надвишават средно установената стойност на активите за отделен клиент на банката;
  - кореспондентски отношения;
  - инкасово обслужване на клиенти, чиято дейност генерира големи парични средства в брой;
  - интернет банкиране, инвестиционни услуги, предлагани на лица извън Европейския съюз и Европейското икономическо пространство.

Рискови фактори, на които се основава преценката за ниво на риск на даден клиент или група от клиенти, са представени в следващата матрица на риска. Освен тях, банката може да определи допълнителни фактори, спрямо които тя извършва преценка в практиката си.

Съществува следната категоризация на рискови фактори, свързани с типа клиент, посочени на диаграмата:



Таблица No 3 Група клиенти, според рисковата категория

Рискова категория	Примери за групи клиенти, според рисковата категория
T1	<p>- кредитна институция от Република България, от друга държава-членка или банка от трета държава, включена в списък, утвърден със съвместна заповед на министъра на финансите и управителя на Българската народна банка;</p> <p>- държавен орган на Република България;</p> <p>- институция, изпълняваща властови функции в съответствие с правото на Европейския съюз при следните условия:</p> <ol style="list-style-type: none"> <li>1. банката е събрала достатъчно информация, която не поражда съмнение за идентичността на институцията;</li> <li>2. институцията спазва процедури за отчетност и дейността е прозрачна;</li> <li>3. институцията се отчита на орган на Общността, на орган на държава-членка или съществуват процедури за проверка, които гарантират контрол на нейната дейност.</li> </ol> <p>- банкова сметка, с титуляр лице по чл. 3, ал. 2, т. 11 и 28, ЗМИП, от Република България, от друга държава-членка или от държава, включена в списъка по чл. 4, ал. 9, ЗМИП при условие, че сметката се използва за депозиране на суми на клиент на титуляра и при условие че идентификацията е извършена и декларацията за произход на средства е приета от титуляра. Отношенията между банката и титуляра на сметката се уреждат по начин, гарантиращ своевременно представяне на цялата информация за клиента на титуляра, при поискване от страна на банката.</p>
T2	<p>- клиент, за който събраната информация преди и след установяване на бизнес отношенията, както и направената оценка на тази база показва, че клиентът не отговаря на критериите за нисък или висок риск</p> <p>- Клиент, за който при текущото прилагане на мерките за комплексна проверка не се констатира отклонения или констатираните отклонения от първоначалната информация за клиента са незначителни.</p>
T3	<p>- Източникът на средства е неясен, неизвестен, клиентът не желае да представи декларация за техния произход;</p>

	<ul style="list-style-type: none"> <li>- Съществуват подозрения, че клиентът действа съобразно указания, давани от трети лица. При посещение в банката, клиентът често е придружаван от трети лица, които го консултират или внимателно следят за изпълнението на операциите;</li> <li>- Операциите се изпълняват по необичаен начин, необясними са основанието, стойността или сложността на транзакциите;</li> <li>- Съществуват индикатори за съмнителни операции, извършвани от клиента (в т.ч. и предишни ДСО до ДАНС, запитвания от ДАНС, прокуратура, полиция);</li> <li>- Клиентът е PEP;</li> <li>- Операциите, отразени по банковата сметка, са свързани с лица, категоризирани от банката като високорискови;</li> <li>- Сред действителните собственици на клиента е лице, категоризирано като PEP;</li> <li>- Юридическо лице, регистрирано в офшорна зона;</li> <li>- Клиент със сложна структура на собственост, при която трудно се установява действителния собственик;</li> <li>- Клиент, за който банката е получила указания от компетентен орган, за замразяване на средствата, блокиране на транзакции (съобразно ЗМИП и ЗМФТ) или за постоянно наблюдение на операциите;</li> <li>- Клиентът фигурира в списъците на ЕС за налагане на ограничителни мерки съобразно резолюциите на ООН за санкциониране на действия, свързани с разпространяване на оръжия за масово унищожаване и терористични действия.</li> </ul>
--	--

#### Рискови фактори, свързани с високо рискови бизнес отношения

КО	Кореспондентски отношения с банка – респондент от трета държава (държава извън ЕС и списъка по чл. 4, ал. 9 от ЗМИП)
----	--

Рискови фактори, свързани с географския регион, а именно като място на постоянна или временна адресна регистрация за физическо лице или в случай на юридическо лице - седалище по регистрация, място на извършване на основния бизнес, място на бизнес-партньорите на клиента. В следващата таблица е дадена примерна категоризация на държави, за които се счита, че са носители на висок риск.

Таблица No 4 – Категоризация на високо рискови държави

Категория	Примери на държави, носители на висок риск
Г1	Държави, спрямо които ЕС прилага ограничителни мерки
Г2	Държави, включени в документите на FATF като некооперативни държави или държави, неприлагащи в достатъчна степен или изцяло международните стандарти за превенция
Г3	Държави, спрямо които Европейският надзорен орган е изразил притеснения за адекватното прилагане на международните стандарти за превенция

Рискови фактори, свързани с ползваните продукти и услуги, предлагани от банката

Таблица No 5 – Рискови фактори, произтичащи от използвани продукти и услуги

<b>Рисков Фактор</b>	<b>Примери за банкови продукти и услуги, носители на висок риск</b>
П1	Продукти, осигуряващи възможност за висока степен на анонимност, осъществяване на трансфер на парични средства извън рамките на ЕС от клиент без физическото му присъствие в банката (интернет банкиране)
П2	Типът на банковата сметка допуска извършване на операции, които не са характерни за този вид сметки (напр. спестовни сметки, често използвани за извършване на разплащания)
П3	Частно банкиране

### Определяне на рисковата група на клиента съобразно рисковите фактори

Таблица No.6 – Определяне на рисковата група

<b>Категория на риска</b>	<b>Код на риска</b>	<b>Рисков фактор</b>
Нисък	А	Клиенти със статус Т1. Прямо тях банката може да прилага опростени мерки за комплексна проверка.
Нормален	В	В категорията попадат клиенти със статус Т2.
Висок	С	В категорията попадат клиенти на които е определен следния статус: <ul style="list-style-type: none"> <li>- Т3</li> <li>- Г1-Г3</li> <li>- КО</li> <li>- П1, П2 и П3</li> </ul>

### 2.4 Мониторинг и анализ на операциите и сделките на клиента

Текущото наблюдение е съществен елемент за ефективно контролиране и намаляване на риска. За целта е необходимо банката да разполага с актуална информация за обичайната дейност на клиента, така че да е в състояние да идентифицира операции, които попадат извън рамките на изградения клиентски профил.

Разбира се, обхватът на наблюдението ще зависи от рисковата категория, в която е класифициран клиентът. Банките трябва да обръщат специално внимание на всички сложни, необичайно големи транзакции и на всички необичайни типове операции, които нямат очевиден икономически и правен смисъл. За определена категория сметки, банката може да определи в правилата си прагове и да наблюдава с повишено внимание всички транзакции, надвишаващи тези прагове. Операции, свързани с големи суми в брой, които не са характерни за обичайния бизнес на клиента, трябва да привлекат вниманието на банковия служител. Сметки, по които ежедневно се поддържа

символична наличност в сравнение с големите по размер операции, отразени по сметката, следва също да са обект на задълбочен анализ, тъй като такива сметки често се използват като „транзитни“. Обект на интензивно наблюдение са сметки на клиенти, определени като високорискови. Всяка банка определя ключови индикатори за такъв вид сметки, като например – произход на средствата, вид на операциите, място на извършване на дейността и др. Банката изгражда и разполага със система за периодичен преглед на различните сметки по рискови категории на клиенти.

Банката се задължава текущо да прилага подходящи мерки за комплексна проверка (МКП), за да може своевременно да открива клиенти и операции, за които възниква съмнение за изпиране на пари или финансиране на тероризъм. Мерките се прилагат спрямо всички клиенти. Обхватът на мерките зависи от рисковия профил на всеки клиент и са представени в таблица No 7:

Таблица No 7 – Обхват на мерките за комплексна проверка

Рискова категория	Код на рисковата категория	Обхват на МКП	Честота на прилагане на МКП
Нисък риск	A	Опростени МКП	веднъж годишно
Нормален риск	B	Стандартни МКП	На всеки 4-6 месеца
Висок	C	Разширени МКП	Ежемесечно

### **3. Управление на риска, на който банката е изложена в областта на превенцията на изпирането на пари и финансирането на тероризъм**

Банката се задължава да управлява всички рискове свързани с дейността ѝ, с цел тяхното минимизиране. В този смисъл, банката разработва и прилага система за управление на риска от изпиране на пари и финансиране на тероризъм, която включва:

- разработени процеси за идентифициране на съществуващи рискове или на потенциални рискове, които могат да възникнат от установяване на отношения с нова клиентска група, от предлагане на нови продукти и услуги;
- ясно определени правомощия и отговорности за управление на риска;
- анализ на риска;
- измерване на риска чрез създаване на механизми и процедури;
- ефективна и надеждна информационна система;
- контрол и намаляване на риска;
- процедура за начин и честота на представяне на информацията на Съвета на директорите или Управителния съвет на банката.

Службите за вътрешен контрол и специализираните служби за превенция играят важна роля при подготовката и прилагането на банковата политика и на процедурите. Като правило, службата за вътрешен контрол трябва да осигури независима оценка на политиките и процедурите на банката, включително на тяхното съответствие с правната и регулаторна рамка. Съставът на службата включва високо компетентни лица, с опит в банковото дело. Вътрешните одитори инспектират правилното прилагане на процедурите в банковите клонове и отразяват всички несъответствия при тяхното прилагане. Докладите с констатациите и препоръките за предприемане на мерки срещу нарушенията на ЗМИП, ППЗМИП и Вътрешните правила, заедно с обясненията и/или

възраженията на ръководителя на проверявания обект на банката, се представят на мениджмънта на банката.

#### *Ръководител на специализираната служба*

Банката определя лице на ръководна длъжност, което ръководи и отговаря за организацията на дейността на специализираната служба по чл. 6, ал. 5 от ЗМИП. Лицето осъществява връзката между банката и БНБ, САД „Финансово разузнаване”, правоохранителните органи, прокуратурата и другите институции, участващи в противодействието на процеса на изпиране на пари и финансиране на тероризма. Ръководителят на специализираната служба отговаря за своевременното изпращане на доклади за съмнителни операции и лица до САД „Финансово разузнаване”, ДАНС и МВР съобразно изискванията на ЗМИП и ЗМФТ.

#### *Съхраняване на информация от банката*

Въвежда се система за съхраняване на информацията по подходящ и надежден начин, който да дава възможност за възстановяване на отделните транзакции и на съдържащата се в тях информация, за целите на разследване на деяния, свързани с изпиране на пари или финансиране на тероризъм.

Съхранява се следният минимум данни, отнасящи се до отделните транзакции:

- вальор на транзакцията и датат на нейното отразяване в счетоводната система на банката;
- референтен номер на транзакцията и уникален регистрационен номер на платежния документ;
- наредител и получател по транзакцията – наименование, номер на сметка, адрес (съобразно изискванията на Регламент 1781/2006/ЕО и съответната платежна система);
- код или наименование на банката на наредителя и на банката на получателя;
- вид на транзакцията;
- данни относно плащането;
- размер на транзакцията.

Посочените елементи на съхраняваната информация са обяснени в съответните раздели на Наредба №3 на БНБ, отнасящи се до съдържанието на платежно нареждане.

Данните за клиентите, документите за извършените операции и сделки, както и посочения по-горе минимум от информация се съхраняват за срок от пет години. Всяка банка предприема подходящи стъпки за разработване на система за съхраняване на информацията, така че същата да може да се извлича по лесен и бърз начин при поискване от компетентните органи.

### **3.1 Управление на риска при изпълнение на парични преводи**

Банките използват паричните преводи като метод за трансфер на суми между техни клиенти. Паричните преводи включват както транзакции на територията на Европейската общност, така и трансфери извън рамките на Общността. Тъй като този вид преводи не включва физическо придвижване на валута, той се счита за бърз и сигурен метод за трансфер на парични стойности от едно място до друго.

Паричният превод е операция, осъществена от името на наредител (физическо или юридическо лице) чрез банка (или платежна институция) по електронен път, с цел да се доставят парични средства на получател (бенефициент) в друга или в същата банка (или платежна институция). Наредителят и получателят могат да бъдат едно и също лице. Предвид целите на настоящите указания, платежните институции няма да бъдат обхванати, въпреки че в значителната си част разпоредбите за осъществяване на парични преводи са в сила и за тях.

Превод извън рамките на Общността, следва да се разбира в смисъла, определен в чл. 7 от Регламент 1781/2006/ЕО и представлява паричен превод, при който едната от двете институции - банката на наредителя или банката на получателя е базирана в държава, извън границите на Европейската общност. Той може да включва участието на една или повече посреднически институции.

Превод в рамките на Общността е определен в чл. 6 от Регламент 1781/2006/ЕО и означава паричен превод, при който банката на наредителя и банката на получателя са базирани на територията на Европейската общност. Той също може да включва участието на посреднически институции.

Паричният превод е незабавен и най-предпочитан начин за трансфер на средства. Затова е необходимо да се изградят защитни системи срещу използването на паричните преводи за финансиране на терористични действия и за изпиране на пари. За целта е необходимо да се осигури предаването на основната информация за наредителя от банката-наредител до банката-получател. По този начин, при възникване на съмнение, цялата налична информация може да бъде предадена на САД „Финансово разузнаване”, ако съмнението не отпадне.

Преводи извън рамките на Общността трябва да включват елементите, определени в Регламент (ЕО) № 1781/2006 на Европейския парламент и на Съвета. Всеки превод трябва да бъде съпроводен от точна и съдържателна информация за наредителя. Информацията трябва да съдържа името, адреса и номера на сметката на наредителя. Адресът може да бъде заместен с дата и място на раждане на наредителя, с клиентски номер или с национален идентификационен номер. Когато наредителят няма банкова сметка, се посочва уникален идентификационен номер, който дава възможност да се проследи транзакцията, за да се получи необходимата информация за платеца. Когато паричните преводи се осъществяват чрез batch file, пълната информация за платеца се посочва само във файла и не е задължително да съпътства всеки индивидуален трансфер, включен в batch file.

За преводи, осъществявани в рамките на Общността, Регламентът допуска за достатъчно посочването на номер на банковата сметка на наредителя или на уникален идентификационен номер, който дава възможност за лесно установяване на наредителя. Институцията на получателя обаче има право да поиска от институцията на наредителя, и последната се задължава да й предостави, пълната информация за наредителя в рамките на три работни дни от получаване на искането.

*Изключения.* Горепосаните изисквания не се отнасят за междубанкови трансфери, при които наредителят и получателят са банки.

*Роля на банката-наредител, посредническата институция и банката-получател, определени в Регламент 1781/2006/ЕО*

Банка-наредител е изпълняващата институция на наредителя на паричния превод. Банката-наредител трябва да осигури наличието на цялата задължителна информация за наредителя, която съпътства паричния превод. Банката трябва също да потвърди и да съхранява информацията за период не по-малък от пет години.

Посредническата институция, която посредничи при изпълнението на парични преводи, както при преводи в рамките на, така и при преводи извън рамките на Общността, трябва да осигури предаването на цялата информация за наредителя, подадена от банката-наредител. Когато съществуват технически пречки за предаване на цялата информация за наредителя, посредническата институция трябва да запази информацията за период от пет години.

Банката-получател трябва да разполага с ефективни процедури, базирани на риска, за да установи своевременно парични преводи, при които информацията за наредителя липсва или е непълна. Липсата или непълнотата на информацията за платеца може да послужи като основание на банката-получател да върне превода или да поиска допълнителна информация за наредителя. Когато банката-наредител редовно не изпълнява задълженията си за изпращане на изискваната информация за платеца, банката-получател предприема няколко стъпки, като първоначалните са изпращане на предупредително писмо и определяне на краен срок за получаване на липсващата информация. След изтичане на крайния срок, банката-получател може да ограничи или да откаже последващо получаване на преводи от банката-наредител, или да прекрати отношенията с неизрядната банка-наредител, като същевременно изпраща доклад до САД „Финансово разузнаване“ за този факт.

При подготовката на правила за извършване на парични преводи, банката може да ползва документът, подготвен от Работната група към трите комитета - Комитета на европейските банкови надзорници, Комитета на европейските надзорници по застраховане и доброволно осигуряване и Комитета на европейските регулаторни органи за ценни книжа, и публикуван на Интернет страницата на БНБ, под заглавие Общо съгласие за задълженията, произтичащи от Европейския регламент 1781/2006 относно информацията за платеца, съпътстваща паричните преводи, към доставчиците на платежни услуги на получателя.

### **3.2 Управление на риска при въвеждане на новите технологии**

Адекватно управление на риска в областта на превенцията срещу изпирането на пари и финансирането на тероризма изисква от банката да минимизира риска, който възниква при въвеждане на новите технологии (интернет банкиране, електронни пари), даващи възможност за анонимност. В тези случаи могат да се приложат допълнителни мерки, като например:

- клиент, ползващ интернет банкиране трябва да присъства лично (за ФЛ) или чрез упълномощен представител (за ЮЛ) по време на идентификацията и проверката на неговата идентичност;
- извършване на допълнителни проверки, с цел недопускане представяне на фалшиви документи (проверка на интернет страницата на МВР за валидност на документа за самоличност);
- защитни системи, които осигуряват безопасно интернет банкиране – използване на PIN, пароли, електронен сертификат.

### **4. Обучение на банковите служители**

Важен елемент в изграждането на ефективна система за превенция срещу изпирането на пари и финансирането на тероризъм е провеждането на подходящо и навременно обучение на банковите служители. Целите на обучението са многостранни. Обучението

трябва да бъде ориентирано както към запознаване с правната рамка, така и към специфичните професионални задължения на служителите. В този смисъл, техниките за превенция, които касиерите следва да прилагат, няма да са идентични с техниките, прилагани от служителите, изпълняващи презгранични парични преводи. По време на обучението се представят: съществуващите законови изисквания; нови тенденции в областта на превенцията; указания и изследвания, издадени от надзорните органи, от международни организации или от банката; дискутират се конкретни казуси, за да се развият професионалните умения на служителите.

Всеки новопостъпил служител трябва да бъде запознат с националната и международна правна рамка за превенция срещу изпиране на пари и финансиране на тероризъм, и с Вътрешните правила на банката, приети на основание чл. 16 от ЗМИП.

Банката трябва да разполага с адекватни механизми за преценка и последващо наблюдение на новоназначените служители, с цел недопускане криминални елементи да използват ресурсите на банката.

Особено внимание се обръща на обучението на служителите от специализираното звено за превенция в банката. Банката следва да осигури възможност на тези служители да посещават различни форми на обучение, провеждани от съответния надзорен орган, от международно признати организации и институции, от Европейската комисия, Световна банка, МВФ и др. Участието в такива форуми допринася за допълнителна информираност на служителите относно новите схеми, прилагани от криминалните елементи, и за новите техники за ефективна превенция, което от своя страна следва да намери отражение в правилата и процедурите на банката.

Ръководството на банката също трябва да бъде информирано, чрез регулярни обучения, за негативните правни, репутационни и оперативни последици, които могат да възникнат, ако системите за контрол не съответстват на законовите изисквания и служителите на банката не са добре обучени.

Информацията за провеждани обучения (в т.ч. материалите за обучение, програма, участници, оценка на знанията) се съхраняват в банката и се представят на надзорния орган при поискване.

***Банките следва да прилагат настоящите указания от 01.07.2012 г.***

## ДЕКЛАРАЦИЯ

Долуподписаният/ата: .....,  
(име, презиме, фамилия)

ЕГН /ЛНЧ/.....,

Дата и място на раждане.....,

Постоянен адрес: .....,

Гражданство : .....,

Документ за самоличност № .....,

Издаден от: .....

Декларирам, че:

не съм

съм

1. в качеството на лице, заемащо или заемало висша държавна длъжност в Република България или в чужда държава, а именно:

- държавен глава, ръководител на правителство, министър и заместник-министър;
- член на парламента;
- съдия в Конституционен съд, във Върховен съд или на друг висш орган на съдебната власт, чиито решения не подлежат на последващо обжалване освен при изключителни обстоятелства;
- член на Сметната палата;
- член на управителни органи на централната банка;
- посланик или ръководител на дипломатически мисии;
- висш офицер от въоръжените сили;
- член на административен, управителен или надзорен орган на държавни предприятия и търговски дружества с едноличен собственик държавата;
- кмет или заместник-кмет на община;
- кмет или заместник-кмет на район;
- председател на общински съвет,

или

2. лице, свързано с лицето по т. 1, а именно:

- съпруг/а или лице, живеещо във фактическо съпружеско съжителство;

- низходящите от първа степен и техните съпрузи или лица, с които живеят във фактическо съпружеско съжителство;
- възходящите от първа степен;
- лице, което е действителен съсобственик съвместно с лицето по т. 1 на юридическо лице или се намира в близки търговски, професионални или други делови отношения с това лице;
- лице, което е едноличен собственик или действителен собственик на юридическо лице, основано в полза на лицето по т. 1.

Известна ми е наказателната отговорност за деклариране на неверни обстоятелства по чл. 313 от Наказателния кодекс.

Дата на деклариране: .....

Декларатор:.....

(подпис)