**11.**

**МЕРКИ СРЕЩУ ИЗПИРАНЕ НА ПАРИ**

Приемането на новия ЗМИП през пролетта на 2018 г. се оказа сериозно предизвикателство за голяма част от бизнеса, попаднал сред многобройните категории от лица, задължени по закон да прилагат мерките за превенция. Имаше и откровено излишни изисквания, като например да се изпращат за одобрение в ДАНС приетите от организациите вътрешни правила за превенция на изпирането на пари. Това изискване отпадна още с предходни изменения в ЗМИП, като в момента задължените субекти следва да актуализират вътрешните си правила съобразно ЗМИП, но не и да ги изпращат в ДАНС. Срокът за актуализирането им дори не е започнал, тъй като за начална дата на 6-месечния срок се счита публикуването на резултатите от Националната оценка на риска от изпиране на пари от ДАНС (все още е в процес на изготвяне). Към момента организациите все пак могат да се водят от наличната наднационална оценка на риска от изпиране на пари, изготвена от Европейската комисия.

На европейско ниво правната уредба динамично се променя и доразвива, като през май беше одобрена т.нар. Пета директива за борба срещу изпирането на пари и финансирането на тероризма.  
  
Очевидни са тенденциите за въвеждане на все по-стриктни правила в тази материя, което налага организациите у нас да изострят вниманието си и да засилят дейността си в тази област.  
  
И след приемането на новия Закон за мерките срещу изпирането на пари духът и основните положения в материята останаха непроменени, но същевременно се въведоха редица различни изисквания. Ето някои от по-съществените.  
  
**Публичен регистър на действителните собственици на компаниите**   
  
Компаниите следва да идентифицират физическите лица, които са действителните им собственици, както и да ги публикуват по партидите на юридическите лица в Търговския регистър и в регистър БУЛСТАТ. Последно заложеният срок за оповестяване на действителните собственици е 1 февруари 2019 г., като законът задължава да се публикува "подходяща, точна и актуална" информация, което означава, че следва внимателно да се проследява дали физическото лице все още има качеството на действителен собственик и дали друг не го е придобил.  
  
Предвид това от съществено значение е всяка задължена организация да отговори на въпроса: "В момента кои физически лица отговарят на изискванията за действителен собственик?"  
  
**"Действителен собственик"** е винаги физическо лице, което в крайна сметка притежава или контролира юридическо лице или друго правно образование, както и физическо лице, от чието име или за чиято сметка се осъществява дадена операция, сделка или дейност. Според закона индикация за пряко притежаване е налице, когато физическо лице/лица притежава/т акционерно или дялово участие най-малко 25 на сто от юридическо лице или друго правно образувание. Следващата ("Пета AML директива") понижава този праг от 25 на сто до 10 на сто.  
  
На 19 октомври 2018 г. беше публикуван за обществено обсъждане и [проект на правилник за приложение на Закона за мерките срещу изпирането на пари](http://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=3823), чието приемане също е закъсняло.  
  
Проектът съдържа и формуляр на декларацията, оповестяваща действителните собственици.  
  
**Завишено внимание спрямо "видните политически личности"**  
  
Дефиницията за "видни политически личности" беше значително разширена от новата директива, поради което новият ни национален закон определя като такива не само чуждестранните лица, а и местните такива. Законът изброява редица категории длъжностни лица, които попадат в това определение - държавни глави, премиери, министри и зам.-министри, депутати, конституционни и върховни съдии, членове на управителни органи на централни банки, посланици и др. Спрямо тях трябва да бъде прилагана разширена комплексна проверка като клиенти, както и спрямо свързаните с тях лица - роднини, съпрузи или лицата, които живеят във фактическо съжителство. Дори и след като вече не заемат длъжността си, мерките спрямо тях остават приложими, ако не е изминала една година от преустановяване на "важните обществени функции", които са им били възложени. При встъпване в делови взаимоотношения с такива лица законът изисква предварително одобрение от служител на висша ръководна длъжност при задължения субект (банки, кредитни институции, застрахователи, инвестиционни посредници и др.).  
  
Макар законът да не споменава изрично, съгласно директивата отказът от делови взаимоотношения с дадено лице само въз основа на факта, че то е видна политическа личност, противоречи на духа на регулацията и на препоръките на FATF (Financial Action Task Force - Работната група за финансово действие).  
  
**Подход, основан на оценката на риска**  
  
Думата "риск" е една от най-често повтарящите се в новия закон, което не е случайно предвид логиката на самата директива. Това е една от новостите в сферата и докато някои смятат, че подходът, основаващ се на степента на риска, предоставя по-голяма гъвкавост, други виждат това като причина за лутане на задължените организации и затруднения да определят какво точно са длъжни да сторят. Според вида на риска например задължените организации ще могат да прилагат опростена комплексна проверка или пък ще се налага разширена комплексна проверка. В този контекст те ще трябва да си изготвят стройни правила, за да могат да са отчетни пред надзорния орган и да защитят преценките, които са направили.  
  
Може да определим оценката на риска от изпиране на пари като основна мярка за превенция по смисъла на закона. Задълженията за извършване на оценка на риска са изведени като отделна Глава седма от закона – както национална оценка на риска, така и изготвяне на оценка на риска от задължените субекти. Оценките на риска се актуализират периодично, съхраняват се и са достъпни за дирекция "Финансово разузнаване" на ДАНС. Професионалните организации и сдружения ще могат да изготвят оценки на риска от изпирането на пари и финансирането на тероризма на секторно равнище.  
  
**Висши ръководни длъжности и тяхната отговорност**  
  
Законът въвежда понятието "служител на висша ръководна длъжност": длъжностно лице или служител, който притежава достатъчно познания относно рисковата експозиция във връзка с изпирането на пари и финансирането на тероризма и достатъчно висок ранг за вземане на решения, засягащи тази рискова експозиция, като не е необходимо във всички случаи това да бъде орган или член на орган на управление или представителство. Видно от дефиницията, като такова лице би могло да се определи например ръководителят на отдел "Съответствие".  
  
Функциите на служителите на висша ръководна длъжност са разнородни, като заслужава да се отбележи, че за прилагането на опростените комплексни проверки се изисква одобрение от такъв служител. За нарушения на закона са предвидени сериозни глоби за лицата, които отговарят за осъществяването или осъществяват вътрешния контрол по изпълнението на задълженията на организациите.  
  
Новата дефиниция за "служител на висша ръководна длъжност" заслужава внимание и поради отдавна съществуваща норма в Наказателния кодекс (НК) – чл. 253б, която предвижда в немаловажни случаи лишаване от свобода до три години и глоба от хиляда до три хиляди лева за длъжностно лице, което наруши или не изпълни разпоредбите на Закона за мерките срещу изпирането на пари. До момента почти липсва практика по тази разпоредба от НК, но предстои да видим дали новият закон и новата дефиниция няма да доведат до ангажиране на наказателна отговорност, свързана с нарушения на ЗМИП.  
  
**Вътрешни политики и защитата на личните данни**  
  
Задължените организации приемат вътрешни правила за контрол и предотвратяване на изпирането на пари. Тези правила и процедури подлежат на утвърждаване от дирекция "Финансово разузнаване" на ДАНС. Спазвайки ЗМИП, организациите не трябва да пренебрегват и принципите за защита на личните данни. Между двете регулации не съществува конфликт, не са взаимоизключващи се и баланс е възможен. Нещо повече, новите правила срещу изпирането на пари могат да се разглеждат като добър повод да се преразгледат естеството, количеството и източникът на лични данни, които се събират за целите на AML1.  
  
В заключение трябва да се отбележи, че регулаторите често нямат нужния ресурс да осъществяват самостоятелна повсеместна надзорна дейност, затова тенденцията на европейско ниво е да се делегират задължения към поднадзорните субекти. В случая това е с цел по-ефективна борба с прането на пари, но този метод е широко разпространен и беше приложен и в материята, свързана със защитата на личните данни. Общият регламент за защита на личните данни също цели да постигне своеобразна саморегулация – спазване на множество задължения (вкл. за съдействие на субектите на лични данни) от организациите и осигуряване на отчетност относно това спазване. Косвеното прехвърляне на AML задължения обаче тласка организациите към извършване на дейности, които са твърде далеч от техния основен бизнес и са типични по-скоро за правоприлагащи органи на държавна власт. По тази причина съществува вероятност организациите да срещнат сериозни затруднения, да допуснат неволни нарушения и да станем свидетели на активна санкционна дейност.

**Още задължени субекти**  
  
Търговци и посредници в търговията с произведения на изкуството попадат в обхвата на задължените лица. В тази нова категория попадат и художествени галерии и аукционни къщи, когато стойността на сделката или на свързаните сделки възлиза на или надвишава 10 000 евро (или тяхната равностойност). Не е тайна, че този тип сделки е изложен на голям риск от изпиране на незаконно придобито имущество – сделките невинаги са публични, цените са предмет на субективна преценка и подлежат на лесна манипулация, като същевременно могат да се "превъртят" значителни суми за кратко време. Публикуваният доклад "На вашите услуги", изготвен от британския клон на "Трансперънси интернешънъл" от края на октомври т.г., ясно показва, че произведенията на изкуство продължават да са предпочитано средство за преобразуване на нечисти капитали.  
  
В задължените категории лица вече са и тези, които по занятие предоставят услуги за обмяна между виртуални валути (т.нар. криптоборси), както и доставчиците на портфейли, които предлагат попечителски услуги (предоставят услуги за опазване на частни криптографски ключове от името на своите клиенти). В някои отношения контрол по спазване на задължения по ЗМИП спрямо тези категории лица ще се осъществява от Комисията за финансов надзор. Нещо повече - тези две нови категории задължени субекти ще се вписват в публичен регистър, който се води и поддържа от НАП, като редът за това предстои да се конкретизира в наредба на министъра на финансите.  
  
По примера на ЕС в момента в САЩ също настоятелно се обсъжда внесен законопроект, въвеждащ подобни изисквания спрямо търговците на арт произведения.  
  
**Забрана за разкриване или поддържане на анонимни банкови сейфове**  
  
Забранява се откриване или поддържане на анонимни сметки или депозитни сертификати или сметки или депозитни сертификати на очевидно фиктивно име, както и наемане или поддържане на анонимни сейфове или сейфове на очевидно фиктивно име.  
  
**По-ниски прагове за прилагане на мерките за комплексна проверка от издателите на електронни пари и техните представители**  
  
Максималният размер на електронно съхраняваната сума, за която може да не се прави комплексна проверка, пада от 250 евро на 150 евро (или левовата равностойност). Дори това изключение няма да се прилага, когато сумата надвишава левовата равностойност на 50 евро или тяхната равностойност.  
  
**Списък с длъжностите, заемани от видни политически личности, и уведомяване на ЕК за него**  
  
Новата разпоредба предвижда ДАНС да предоставя на Европейската комисия списък на длъжностите, свързани с изпълнението на важни обществени функции. В случай че такива лица са потенциални клиенти, съществуващи клиенти или собственици на дружества, с които организациите осъществяват бизнес отношения, то следва да се пристъпи към разширена комплексна проверка поради по-високия риск. Според закона по-високият риск остава дори и когато лицето вече не заема съответната длъжност – поне за срок от една година. В тази високорискова категория попадат министри, заместник-министри, депутати, кметове. членове на Сметната палата, на централната банка, посланици, висши офицери и др. За изпълнение на задължението централни и местни органи на власт ще предоставят тази информация на ДАНС. Законът предвижда възможността списъкът да бъде оповестен публично, а публичността в голяма степен би улеснила организациите в идентифицирането на тези лица, тъй като в момента практически се разчита основно на декларации от лицата, с които заявяват дали заемат такива длъжности или не.  
  
**По-голямо внимание по отношение на деловите взаимоотношения, операциите и сделките с лица от рискови държави**  
  
През февруари Европейската комисия прие актуализиран [списък на държавите](https://ec.europa.eu/commission/presscorner/detail/bg/MEMO_19_782), които проявяват слабости в борбата с изпирането на пари. С новите изменения в ЗМИП по-категорично се изисква от задължените субекти да събират по-детайлна информация, когато в деловите взаимоотношения е намесено лице от тези държави. При такава ситуация организациите следва да съберат допълнително информация за клиента, собственика му, планирания характер на взаимоотношенията, произхода на средствата и др. Освен това деловите отношения задължително се поставят под текущо и разширено наблюдение, а за да се установят такива отношения, изначално е нужно одобрението на служител на висша ръководна длъжност. За служител на висша ръководна длъжност се приема длъжностно лице или служител, които притежават достатъчно познания относно рисковата експозиция на организацията и имат нужния висок ранг за вземане на решения, засягащи тази рискова експозиция (не е необходимо във всички случаи това да бъде орган или член на орган на управление или представителство).  
  
**Електронна идентификация на контрагенти**  
  
Изрично се разписа възможността идентифицирането на клиента и проверката на идентификационните данни да се извършват и чрез средства за електронна идентификация, съответни удостоверителни услуги, предвидени в Регламент (ЕС) 910/2014 или друг признат с нормативен акт начин за електронна идентификация. Това е положителна конкретизация на така или иначе случващото се в практиката. Самата Пета директива отчита техническите достижения и цифровизацията на сделките, като предвижда това улеснение, без което дистанционните сделки практически не биха могли да се случват.

**Задължения за действителните собственици**  
  
Промените в ЗМИП формулираха изрично задължение за действителните собственици - физически лица, да предоставят на учредените у нас юридически лица и други правни образувания цялата информация, която е необходима, за изпълнение на задълженията им по заявяване на вписване в Търговския регистър или Регистър Булстат. Преди това законът предпоставяше към известно противоречие – от една страна, законният представител на дружеството беше длъжен да заяви за вписване действителния му собственик, а от друга страна – действителният собственик не беше длъжен да даде нужната за това информация. С измененията се способства и помага на добросъвестните юридически лица и други правни образувания да изпълнят задълженията си да обявят действителния си собственик (в случай че такова задължение съществува спрямо тях).  
  
**ЗМИП и личните данни**  
  
Преди установяване на делово взаимоотношение или извършване на случайна сделка или операция задължените субекти предоставят на клиентите информация за целите, за които ще се обработват личните им данни. Това обикновено става с препратка към Политиката за обработване на лични данни/Уведомлението за поверителност. Поради честите запитвания следва да се подчертае, че и досега нямаше законова колизия между ЗМИП и GDPR, тъй като обработването на лични данни за целите на превенцията на изпирането на пари и финансирането на тероризма се смята за въпрос от обществен интерес съгласно GDPR и не може да бъде ограничено от изискванията му. По същата причина ЗМИП предвижда и обмен на информация (включително лични данни) между дружества от една и съща икономическа група, но намиращи се в трети държави, без да са налице общите основания за трансфер на лични данни.

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 й прилагане е другото важно условие за успешни действия.

**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 рисково базирания подход, 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 клиенти 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 транзакциите.

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.

**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.

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 транзакции, 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 Резолюциите 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.

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 регистрация.

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 рисково базирания 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”.

2.3.1.3 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.

**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.

**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.