

ДЪРЖАВНА АГЕНЦИЯ „НАЦИОНАЛНА СИГУРНОСТ”
САД „ФИНАНСОВО РАЗУЗНАВАНЕ”

1320 Банкя, ул. „Патриот“ № 28, тел. 02 814 7951, fid@dans.bg



НАСОКИ ЗА
ПРИЛАГАНЕ НА ЗАДЪЛЖЕНИЯТА ЗА МЕРКИТЕ СРЕЩУ ИЗПИРАНЕТО НА ПАРИ
И ФИНАНСИРАНЕТО НА ТЕРОРИЗМА ЗА ПОЩЕНСКИТЕ ОПЕРАТОРИ,
ЛИЦЕНЗИРАНИ ДА ИЗВЪРШВАТ ПОЩЕНСКИ ПАРИЧНИ ПРЕВОДИ СЪГЛАСНО
ЗАКОНА ЗА ПОЩЕНСКИТЕ УСЛУГИ И ТЕХНИТЕ ПРЕДСТАВИТЕЛИ ПО ЧЛ. 22 ОТ
СЪЩИЯ ЗАКОН, НА КОИТО Е ВЪЗЛОЖЕНО ИЗПЪЛНЕНИЕТО НА ОТДЕЛНИ
ДЕЙНОСТИ ОТ ПОЩЕНСКАТА УСЛУГА, СВЪРЗАНИ С ОСЪЩЕСТВЯВАНЕТО НА
ПОЩЕНСКИ ПАРИЧНИ ПРЕВОДИ

юли 2024 г.

СЪДЪРЖАНИЕ

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ:	3
I. ВЪВЕДЕНИЕ	4
II. ОПРЕДЕЛЕНИЕ ЗА ИЗПИРАНЕ НА ПАРИ	4
II. 1. ФАЗИ НА ИЗПИРАНЕ НА ПАРИ. КОНСТАТАЦИИ В НАЦИОНАЛНАТА ОЦЕНКА НА РИСКОВЕТЕ ОТ ИЗПИРАНЕ НА ПАРИ И ФИНАНСИРАНЕ НА ТЕРОРИЗМА ПО ОТНОШЕНИЕ НА ПОЩЕНСКИТЕ ПАРИЧНИ ПРЕВОДИ	5
II. 2. МЕТОДИ ЗА ИЗПИРАНЕ НА ПАРИ.....	6
II. 3. КЛЮЧОВИ МЕРКИ, КОИТО СЛЕДВА ДА СЕ ВЗЕМАТ ОТ ПОЩЕНСКИТЕ ОПЕРАТОРИ И ТЕХНИТЕ ПРЕДСТАВИТЕЛИ ЗА ИЗПЪЛНЕНИЕ НА ЗАДЪЛЖЕНИЯТА ПО ЗМИП.....	7
III. ОЦЕНКА НА РИСКА И ВЪТРЕШЕН КОНТРОЛ	7
III. 1. РИСКОВО БАЗИРАН ПОДХОД	7
III. 1. 1. Оценка на риска (НОР/Собствена оценка на риска).....	8
III. 1. 2. Ограничаване на риска	10
III. 1. 3. Наблюдение на риска.....	11
IV. ВЪТРЕШЕН КОНТРОЛ.....	11
IV. 1. 1. ВЪТРЕШНИ ПРАВИЛА ЗА КОНТРОЛ И ПРЕДОТВРАТЯВАНЕ ИЗПИРАНЕТО НА ПАРИ И ФИНАНСИРАНЕТО НА ТЕРОРИЗМА ПО ЧЛ. 101 ОТ ЗМИП	11
IV. 1. 2. Определяне на лице, което да осъществява вътрешния контрол по изпълнението на задълженията, определени в ЗМИП, ППЗМИП и ЗМФТ	12
IV. 1. 3. Обучение.....	12
V. КОМПЛЕКСНА ПРОВЕРКА НА КЛИЕНТА (КПК)	13
V. 1. МОМЕНТ НА ИЗВЪРШВАНЕ НА КОМПЛЕКСНАТА ПРОВЕРКА НА КЛИЕНТА	13
V. 2. МЕРКИ ЗА ИЗВЪРШВАНЕ НА КОМПЛЕКСНА ПРОВЕРКА НА КЛИЕНТА	13
V. 2. 1. Опознаване на клиента – идентификация, действителна собственост, произход на средства и имуществено състояние (богатство), наблюдение.....	13
V. 3. ВИДНИ ПОЛИТИЧЕСКИ ЛИЧНОСТИ (ВПЛ)	14
V. 4. РАЗШИРЕНА КОМПЛЕКСНА ПРОВЕРКА	14
V. 5. ОПРОСТЕНА КОМПЛЕКСНА ПРОВЕРКА.....	15
VI. ТЕКУЩО И РАЗШИРЕНО НАБЛЮДЕНИЕ	16
VI. 1. ТЕКУЩО НАБЛЮДЕНИЕ	16
VI. 2. РАЗШИРЕНО НАБЛЮДЕНИЕ – ВПЛ, ВИСОКОРИСКОВИ ДЪРЖАВИ, ТРАНСГРАНИЧНИ СДЕЛКИ И КЛИЕНТИ	16
VII. УВЕДОМЯВАНЕ ЗА СЪМНИТЕЛНИ СДЕЛКИ/ОПЕРАЦИИ/КЛИЕНТИ	16
VIII. СЪХРАНЯВАНЕ НА ИНФОРМАЦИЯ	18
VIII. 1. СРОК ЗА СЪХРАНЯВАНЕ НА ИНФОРМАЦИЯ.....	18
IX. ЧУЖДЕСТРАННИ КЛОНОВЕ И ДЪЩЕРНИ ДРУЖЕСТВА	19
IX. 1. ИЗИСКВАНИЯ ЗА ПРИЛАГАНЕ НА МЕРКИТЕ СРЕЩУ ИП/ФТ, ПРИЛОЖИМИ КЪМ ЧУЖДЕСТРАННИ КЛОНОВЕ И ДЪЩЕРНИ ДРУЖЕСТВА	19
X. ЦЕЛЕВИ ФИНАНСОВИ САНКЦИИ ЗА ФИНАНСИРАНЕ НА ТЕРОРИЗМА	19
XI. ИСКАНИЯ ЗА ИНФОРМАЦИЯ ОТ САД ФР – ДАНС	20
XI. 1. ИСКАНИЯ ЗА ИНФОРМАЦИЯ ОТ САД ФР – ДАНС ВЪВ ВРЪЗКА С ОСЪЩЕСТВЯВАНЕ НА КОНТРОЛНА ДЕЙНОСТ	21
XI. 2. ИСКАНИЯ ЗА ИНФОРМАЦИЯ ОТ САД ФР – ДАНС ПО РЕДА НА ЧЛ. 74 ОТ ЗМИП 21	
XI. 3. ПРОВЕРКА НА МЯСТО.....	21

XI. 4. САНКЦИИ ЗА НЕСПАЗВАНЕ НА МЕРКИТЕ СРЕЩУ ИЗПИРАНЕТО НА ПАРИ ИЛИ ФИНАНСИРАНЕТО НА ТЕРОРИЗМА	22
XII. ЗАКЛЮЧЕНИЕ	22
ПРИЛОЖЕНИЕ 1– Рискове, свързани с клиента, предлаганите услуги и географски риск за пощенските оператори и техните представители	23
Географски фактори.....	23
Риск, свързан с клиента	23
Рискове, свързани със сделката	24
ПРИЛОЖЕНИЕ 2 – Мерки за ограничаване на риска.....	25
ПРИЛОЖЕНИЕ 3 - примерен списък с критерии за съмнение, който пощенските оператори и техните представители могат да ползват.	26
ПРИЛОЖЕНИЕ 4 - Списък с методически указания, насоки и друга полезна информация	28

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ:

ВПЛ	Видна политическа личност
ЗМИП	Закон за мерките срещу изпирането на пари
ЗМФТ	Закона за мерките срещу финансирането на тероризма
ППЗМИП	Правилник за прилагане на закона за мерките срещу изпирането на пари
ИП	Изпиране на пари
ФТ	Финансиране на тероризъм
МИП/МФТ	Мерки срещу изпирането на пари/ финансирането на тероризъм
КПК	Комплексна проверка на клиента
ЕС	Европейски съюз
FATF ¹	Групата за финансови действия срещу изпирането на пари
САД ФР – ДАНС	Специализирана административна дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“
НОР	Национална оценка на риска
УСО	Уведомление за съмнителна операция

¹ Групата за финансови действия срещу изпирането на пари (Financial Action Task Force/FATF) – междуправителствена организация, създадена с Решение на държавните глави на страните от Г-7 и председателя на Европейската комисия по време на срещата на върха на Г-7, състояла се в Париж през 1989 г.

I. ВЪВЕДЕНИЕ

Тези насоки са разработени от САД ФР – ДАНС в съответствие с чл. 16, ал. 3, т. 2, б. „б“ от ППЗМИП в полза на пощенските оператори, лицензирани да извършват пощенски парични преводи съгласно Закона за пощенските услуги и техните представители по чл. 22 от същия закон, на които е възложено изпълнението на отделни дейности от пощенската услуга, свързани с осъществяването на пощенски парични преводи (задължени субекти по чл. 4, т. 7 от ЗМИП).

За подготвяне на настоящите насоки са използвани документи, специално изготвени от международен експерт и предоставени на българските институции от Съвета на Европа във връзка с проект, финансиран по Програмата за подпомагане на структурните реформи (ППСР) на Европейската комисия, имащ за цел да повиши възможностите на българските власти за ефективно ограничаване на рисковете от изпиране на пари (ИП) и финансиране на тероризъм (ФТ), чрез осигуряване на техническо съдействие от Съвета на Европа.

Настоящите насоки отразяват последните измененията и допълнения на превантивното законодателство на Република България срещу изпирането на пари и финансирането на тероризма.

Насоките са разработени, за да се подпомогнат пощенските оператори, лицензирани да извършват пощенски парични преводи съгласно Закона за пощенските услуги и техните представители по чл. 22 от същия закон, на които е възложено изпълнението на отделни дейности от пощенската услуга, свързани с осъществяването на пощенски парични преводи:

- да установяват, разбират и оценяват рисковете от изпиране на пари и финансиране на тероризъм;
- да прилагат мерките за комплексна проверка;
- да установяват произхода на средствата, използвани в конкретното делово взаимоотношение, сделка или операция;
- да установят източника на богатството на клиент видна политическа личност или на свързаното на такава личност лице;
- да прилагат правилата за встъпване, продължаване или наблюдение на взаимоотношенията с клиент ВПЛ или свързано на такава личност лице;
- да идентифицират действителните собственици и да разбират и оценяват свързаните с тях рискове;
- да прилагат нормативните изисквания, свързани с целевите финансови санкции;
- да подобрят разпознаването на съмнителни операции, сделки и клиенти спрямо индивидуалния рисков профил и да подобрят качеството на подаваните уведомления към САД „Финансово разузнаване“ - ДАНС.

II. ОПРЕДЕЛЕНИЕ ЗА ИЗПИРАНЕ НА ПАРИ

Съгласно чл. 2 от ЗМИП, изпирането на пари, когато е извършено умишлено, е:

1. преобразуването или прехвърлянето на имущество, със знанието, че това имущество е придобито от престъпление или от акт на участие в престъпление, 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 се избегнат правните последици от деянието на това лице;

2. укриването или прикриването на естеството, източника, местонахождението, разположението, движението, правата по отношение на или собствеността върху имущество, със знанието, че това имущество е придобито от престъпление или от акт на участие в престъпление;

3. придобиването, владението, държането или използването на имущество със знание към момента на получаването, че е придобито от престъпление или от акт на участие в престъпление;

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, улесняването или даването на съвети при извършването на такова действие или неговото прикриване.

5. Изпиране на пари е налице и когато престъплението, от което е придобито имуществото по т. 1 – 4 е извършено в друга държава членка или в трета държава и не попада под юрисдикцията на Република България.

Престъпната дейност винаги предхожда престъплението изпиране на пари, това е укриването на истинския източник на постъпленията от престъплението и цялото имущество, получено от тези постъпления.

II. 1. ФАЗИ НА ИЗПИРАНЕ НА ПАРИ. КОНСТАТАЦИИ В НАЦИОНАЛНАТА ОЦЕНКА НА РИСКОВЕТЕ ОТ ИЗПИРАНЕ НА ПАРИ И ФИНАНСИРАНЕ НА ТЕРОРИЗМА ПО ОТНОШЕНИЕ НА ПОЩЕНСКИТЕ ПАРИЧНИ ПРЕВОДИ

Процесът на изпиране на пари може да се опише в три фази:

- Влагане: средства, получени от престъпни дейности (например търговия с наркотици), се въвеждат (влагат) за първи път във финансовата система или се използват за закупуване на стоки или имущество с висока стойност.

- Разслояване: в тази фаза средствата се разслояват и се включват във финансови потоци чрез използване на множество и/или сложни сделки. Извършването на сложни сделки е опит да се прикрие по различни начини източникът на незаконно придобитите средства или собственикът на средствата.

- Интеграция – вливане на финансовите средства активи в реалната икономика.

Съгласно актуализираната Национална оценка на риска (публикувана на интернет страницата на ДАНС, в раздел „Дейности“, подраздел „Мерки срещу изпирането на пари и финансирането на тероризъм“, секция „Национална оценка на риска“), пощенските парични преводи представляват среден риск, тъй като се установява използването на оператори, предоставящи услугата „пощенски паричен превод“ (в т.ч. и услугата „наложен платеж“), в редица типологии за изпиране на пари, главно имащи за цел прехвърляне на средства с неясен произход, както и в някои типологии за финансиране на тероризъм, главно имащи за цел прехвърляне на средства с неясно предназначение, както и получаване на средства в резултат

на измама. Сходните характеристики на пощенските парични преводи с тези на наличните парични преводи, също излагат сектора на някои рискове от ИП/ ФТ. В тази връзка особено внимание е необходимо в случаите на трансгранични преводи, както и предвид възможността за използването им за прехвърляне на средства, включително такива, асоциирани с мигрантски общности в Република България, като съществуват признаци за връзка на същите с ФТ.

II. 2. МЕТОДИ ЗА ИЗПИРАНЕ НА ПАРИ

Наред с технологичното развитие нараства и броят на усъвършенстваните и сложни методи, използвани за прикриване произхода на незаконно придобито имущество. Съществуват множество методи, но следните са някои от най-често използваните от „перачите“, които се опитват да заобиколят разкриването:

Фалшиви компании – т. нар. „кухи фирми“ прикриват изпраните средства, докато „светлите фирми“ извършват законни бизнес дейности, за да прикрият изпирането на пари. Този метод често се използва във фазата на наслояване, като самата процедура за изпиране на пари може да се проведе в няколко държави.

Използване на подставени лица – това е най-често използваният метод за изпиране на пари на етапа на Вложение. Лице, което желае да вкара „мръсни пари“ във финансовата система, може да се опита да прикрие произхода на незаконно придобито имущество, като ангажира „подставени лица“, напр. членове на семейството, приятели или бизнес партньори, които се ползват с доверието на общността и извършват трансакции от негово име.

Структуриране – т. нар. „смърфинг“, което представлява структуриране на по-големи суми пари в брой, над законодателния праг за водене на записи и отчитане, в – парични трансакции с по-малък размер с цел въвеждането им във финансовата система. Перачът може да използва много „смърфинг“, за да структурира „мръсните“ си пари. Като структурира по-големия паричен депозит в по-малки депозити, често депозирани от много „смърфове“, перачът се опитва да избегне няколко метода за разкриване, създадени като част от режима за противодействие на изпиране на пари/финансиране на тероризма, като например задължението за уведомяване за парични трансакции над определена сума в наличност и задължението за идентифициране на клиента. Поради тези причини „смърфингът“ често се използва в процеса на ИП/ФТ.

Покупка на имущество с пари в брой – пощенските парични преводи под формата на наложен платеж могат да послужат при закупуването на вещи на значителна стойност и заплащането им в брой.

Рафиниране – по-малки деноминации на незаконно придобити средства, като средства, придобити чрез улично разпространение на наркотици, биха могли да се използват за разплащане при сделки с наложен платеж.

Пощенските оператори и техните представители трябва да се позовават на различни източници като насоки от САД ФР – ДАНС, информация от техните професионални организации и да поддържат познанията си за тенденциите и типологиите на изпирането на пари от САД ФР – ДАНС (<http://www.dans.bg>), FATF (<http://www.fatf-gafi.org/>) и други международни органи.

II. 3. КЛЮЧОВИ МЕРКИ, КОИТО СЛЕДВА ДА СЕ ВЗЕМАТ ОТ ПОЩЕНСКИТЕ ОПЕРАТОРИ И ТЕХНИТЕ ПРЕДСТАВИТЕЛИ ЗА ИЗПЪЛНЕНИЕ НА ЗАДЪЛЖЕНИЯТА ПО ЗМИП

Ефективен режим за предотвратяване и разкриване на ИП/ФТ е този, при който пощенските оператори и техните представители:

- спазват изцяло своите законови задължения;
- са приспособили своите бизнес операции за превенция на рисковете от изпиране на пари/финансиране на тероризма;
- последователно прилагат мерките за превенция на изпирането на пари и финансирането на тероризма; и
- отговарят на съществуващите международни и национални стандарти за превенция на изпирането на пари и финансирането на тероризма.

За да могат пощенските оператори и техните представители да разберат по-добре и да постигнат съответствие със задълженията си съгласно Закона за мерките срещу изпирането на пари (чл. 3 от ЗМИП и чл. 3 от ЗМФТ), тези насоки са групирани както следва:

- Установяване, разбиране и оценяване на рисковете, свързани с изпирането на пари и финансирането на тероризма, както и мерките за вътрешен контрол;
- Комплексна проверка на клиента;
- Текущо и разширено наблюдение;
- Разкриване на информация при съмнение за изпиране на пари;
- Съхранение на данни и архивиране; и
- Целеви финансови санкции за финансиране на тероризъм.

Във всяка от тези категории са предоставени подробни насоки за изискванията, които трябва да бъдат изпълнени от пощенските оператори и техните представители.

III. ОЦЕНКА НА РИСКА² И ВЪТРЕШЕН КОНТРОЛ

III. 1. РИСКОВО БАЗИРАН ПОДХОД

Рисково базиран подход означава обхватът на прилаганите мерки за предотвратяване и разкриване на изпирането на пари и финансирането на тероризма да бъде пропорционален на установената степен на риск от изпиране на пари и финансиране на тероризма.

Пощенските оператори са длъжни да извършват оценка и документиране на рисковете, свързани с изпирането на пари и финансирането на тероризма. Рисково базираният подход е процес, който позволява на пощенските оператори да идентифицират потенциално високи рискове от изпиране на пари и финансиране на тероризма и да разработят стратегии за тяхното смекчаване. Когато става въпрос за ситуации, в които е подходяща разширена комплексна проверка, принципът на рисково базираният подход ще позволи на пощенските оператори и техните представители да съсредоточат ресурсите там, където са най-необходими за

² Риск – вероятността и въздействието от осъществяване на изпиране на пари/финансиране на тероризъм

управление на рисковете в рамките на допустимото ниво на пощенския оператор или неговия представител.

Необходими са три стъпки за установяване на рисково базиран подход: оценка на риска, смекчаване на риска и наблюдение на риска.

III. 1. 1. Оценка на риска (НОР/Собствена оценка на риска)

Собствената оценка на риска е част от Вътрешните правила за контрол и предотвратяване изпирането на пари и финансирането на тероризма по чл. 101 от ЗМИП.

Съгласно чл. 101, ал. 8 от ЗМИП представителите на лицензираните пощенски оператори са длъжни да спазват и прилагат вътрешните правила, приети от лицензирания пощенски оператор, от името на когото осъществяват дейността си.

От своя страна лицензираният пощенски оператор е длъжен да наблюдава спазването на правилата от страна на неговите представители.

Собствената оценката на риска е анализ на потенциални заплахи и уязвимости от изпиране на пари и финансиране на тероризма, на които е изложен бизнесът на пощенския оператор или неговия представител. Сложността на оценката зависи от размера и рисковите фактори, свързани с бизнеса на пощенските оператори и техните представители.

Оценката на риска, извършвана от пощенските оператори, трябва да вземе предвид резултатите от Националната оценка на риска (НОР), извършена от постоянно действащата междуведомствена работна група по чл. 96, ал. 1 от ЗМИП. Актуализирана НОР е продукт на съвместни действия на правоохранителни органи, органи по национална сигурност, прокуратурата, органи за надзор, други държавни органи и частния сектор и отразява предоставената от тях информация. Източниците на информация включват и публични национални и международни доклади в съответните области, в т.ч. такива, публикувани от ЕВРОПОЛ, Групата за финансови действия срещу изпирането на пари (FATF), Комитета Монивал към Съвета на Европа, както и Наднационалната оценка на риска от изпиране на пари и финансиране на тероризъм на Европейската комисия.

Националната оценка на риска установи, че пощенските оператори и техните представители са уязвими към изпиране на пари/финансиране на тероризма поради извършването на платежни операции в брой и възможността за използване на услугите им от криминално проявени лица и техните съучастници.

Основните рискови събития, засягащи пощенските оператори и техните представители са отбелязани в НОР, информация за която е достъпна на интернет страницата на ДАНС. Както се отбеляза по-горе, следва да се отчитат и сходствата на пощенските парични преводи с наличните парични преводи.

При извършване на оценка на риска пощенските оператори трябва да идентифицират и оценят основните рискове от изпиране на пари/финансиране на тероризма в следните категории:

1. Риск, свързан с клиента

Пощенските оператори трябва да вземат предвид естеството и бизнеса на своите клиенти, за да определят нивото на риск от изпиране на пари и финансиране на тероризма.

Приложение 1 предоставя допълнителни примери за клиенти с по-висок риск.

2. Продуктов риск

Пощенските оператори трябва да познават и разпознават продукти и услуги или комбинации от тях, които могат да представляват по-висок риск от изпиране на пари или финансиране на тероризъм. Законните продукти и услуги могат да се използват за маскиране на незаконния произход на средства, за преместване на средства за финансиране на терористични актове или за скриване на истинската самоличност на действителния собственик или бенефициент на продукта или услугата. Продукти и услуги, които могат да поддържат движението и преобразуването на активи във, през и извън финансовата система, могат да представляват висок риск. Освен това може също така да се имат предвид услугите, идентифицирани от регулаторите, правителствените органи или други надеждни източници като потенциално високорискови за изпиране на пари или финансиране на тероризма.

Приложение 1 предоставя допълнителни примери за по-висок риск при пощенските парични преводи.

3. Риск, свързан с бизнес практики/каналите за доставка

От пощенските оператори също се изисква да вземат предвид каналите, използвани за доставка на техните продукти или услуги. В днешната икономика и глобален пазар много канали за доставка не водят клиента до пряк контакт лице в лице със пощенския оператор или неговия представител (например интернет или телефон) и са достъпни 24 часа в денонощието, 7 дни в седмицата, от почти навсякъде. Отдалечеността на някои от тези канали за разпространение може също да се използва за прикриване на истинската самоличност на клиент или действителни собственици и следователно може да създаде по-високи рискове. В този аспект от особено значение за пощенските оператори и техните представители е услугата наложен платеж.

4. Географски риск

Пощенските оператори трябва да преценят дали географските местоположения, в които оперират или осъществяват дейност, представляват потенциално по-висок риск от изпиране на пари и финансиране на тероризма. В зависимост от техния бизнес и операции, географските местоположения могат да варират от непосредствената им среда, до други страни.

Приложение 1 съдържа примерен списък, който пощенските оператори могат да ползват, за да се улесни оценката на горните фактори. Оценката на риска на пощенския оператор обаче трябва да е подходяща за неговите специфични бизнес нужди, което означава, че може да се наложи да бъде по-подробна или различна от предоставения примерен списък. Пощенските оператори могат да персонализират списъка или да използват различен метод или друг инструмент.

По отношение на оценката на риска следва да се прилагат **Насоки за изготвяне на оценка на риска от изпиране на пари и финансиране на тероризма**, публикувани на интернет страницата на ДАНС³.

5. Висок риск от изпиране на пари и финансиране на тероризъм

Въпреки че няма общоприет списък с рискови категории, примерите в Приложение 1 могат да помогнат при определянето на ситуации с по-висок риск. Трябва да се отбележи, че ако се определи че даден клиент или ситуация представлява по-висок риск, от лицето по чл. 4 от ЗМИП се изисква да приложи мерки за ограничаване на риска и разширена комплексна проверка. По-високият риск не води автоматично до задължение да се откаже сделката или да се прекрати деловото взаимоотношение.

6. Променливи рискови фактори, които могат да окажат влияние върху риска

Пощенските оператори следва да се съобразяват с особеностите, степента на риск или съмнителност на дадена сделка или бизнес отношения. Следователно процедурата за оценка на риска може да съдържа и променливи рискове, които са специфични за определен клиент или вид бизнес. Наличието на една или повече променливи може да доведе до прилагането на разширена комплексна проверка и до необходимостта от наблюдение или обичайната комплексна проверка и наблюдение могат да бъдат намалени или опростени. Някои от променливите, които могат да окажат влияние върху повишаването или ограничаването на риска на определен клиент или тип бизнес са:

- естеството на бизнес отношенията с клиента и наличието на специфични дейности;
- ниво на законодателство или наличие на надзор от компетентни органи. Например, клиентите, които са обект на задоволителна система за предотвратяване на изпирането на пари и финансирането на тероризма, представляват по-нисък риск от клиентите от сектори, където има риск от изпиране на пари поради липса на регулация, насочена към предотвратяване на изпирането на пари;
- репутация и публично достъпна информация за клиента. Юридическите лица, които са прозрачни и добре известни в публичното пространство и които работят в продължение на много години, без да има санкции срещу тях (нарушения, свързани с незаконно придобито имущество), представляват нисък риск от изпиране на пари;
- редовност или продължителност на бизнес отношенията;
- познаване на държавата на клиента, включително познаване на местните закони, разпоредби и правила;
- пропорционалност между размера или обхвата и продължителността на дейността на клиента, включително естеството на исканата услуга;

III. 1. 2. Ограничаване на риска

Ограничаване на риска е свързано с прилагането на мерки за ограничаване на потенциалните рискове от изпиране на пари и финансиране на тероризма, които пощенският оператор е идентифицирал, като същевременно остава в рамките на своето ниво на

³ https://dans.bg/upload/344/Pr4_Nasoki_ocenka_na_riska_bul.pdf

толерантност към риска. Като част от своя вътрешен контрол, когато оценката на риска установи, че рисковете са от ИП или ФТ са високи, пощенският оператор трябва да разработи писмени стратегии за ограничаване на риска (политики и процедури, предназначени за ограничаване на високия риск) и да ги приложи за високорискови ситуации. Приложение 2 предоставя списък с мерки за ограничаване на риска, които може да са подходящи за ситуации, които сте определили като по-рискови.

III. 1. 3. Наблюдение на риска

В допълнение към оценката на риска и дейностите по ограничаване на риска, ЗМИП също изисква пощенските оператори и техните представители да предприемат мерки за провеждане на текущо наблюдение. Нивото на наблюдение трябва да бъде адаптирано според рисковете от ИП/ФТ, както е посочено в оценката на риска на пощенския оператор. Целта на текущите дейности за наблюдение е да способства за откриване на съмнителни операции.

Политиките, контролите и процедурите на пощенските оператори трябва да определят какъв вид наблюдение се извършва за конкретни високорискови ситуации, включително как да се открият съмнителни операции. Политиките, контролите и процедурите също трябва да опишат кога се извършва наблюдение (неговата честота), как се преглежда и как ще се прилага последователно.

Пощенските оператори и техните представители могат да използват автоматично или не наблюдение в зависимост от размера и сложността на техните сделки/операции.

IV. ВЪТРЕШЕН КОНТРОЛ

IV. 1. 1. ВЪТРЕШНИ ПРАВИЛА ЗА КОНТРОЛ И ПРЕДОТВРЯВАНЕ ИЗПИРАНЕТО НА ПАРИ И ФИНАНСИРАНЕТО НА ТЕРОРИЗМА ПО ЧЛ. 101 ОТ ЗМИП

Всички пощенски оператори приемат **Вътрешни правила за контрол и предотвратяване изпирането на пари и финансирането на тероризма по чл. 101 от ЗМИП** (вътрешни писмени политики, процедури и механизми за контрол за предотвратяване на изпиране на пари и финансиране на тероризма).

Както се отбеляза по-горе, представителите на лицензираните пощенски оператори са длъжни да спазват и прилагат вътрешните правила, приети от лицензиария пощенски оператор, от името на когото осъществяват дейността си.

От своя страна лицензиарият пощенски оператор е длъжен да наблюдава спазването на правилата от страна на неговите представители, като процедурите за това следва да са част от вътрешните правила.

Политиките, процедурите и механизмите за контрол включват, но не само:

- процедура за комплексна проверка на клиента, включително процедури за идентификация и проверка на клиента, установяване на видни политически личности, действителни собственици, произход на средства, източник на богатство;
- процедура за уведомяване на САД ФР – ДАНС и изпращане на информация, данни и документация към САД ФР – ДАНС;

- процедура за обработка или предприемане на допълнителни действия във връзка със съмнителното действие или операция, включително мерки за предотвратяване на по-нататъшни действия във връзка със съмнително действие или операция;
- определяне на лице, което да осъществява вътрешния контрол по изпълнението на задълженията, определени в ЗМИП, ППЗМИП и ЗМФТ, както и да осигурява условия за тяхната работа;
- организиране и финансиране на програмата за обучение на служителите по задълженията, наложени със ЗМИП;
- създаване на адекватни органи за регулярен вътрешен контрол за изпълнение на задълженията, определени в ЗМИП и одитна функция за тестване на системата за отчетност и идентификация, с изключение на пощенските оператори и техните представители с ограничен брой служители;
- прилагане на индикатори (критерии), в т.ч. и специфични индикатори на пощенския оператор за идентифициране на лица и транзакции, по отношение на които има основание да се подозира изпиране на пари или финансиране на тероризъм;
- процедури за събиране и съхраняване на данни, защита и съхранение на данни в съответствие със закона и процедура за предотвратяване на неототоризиран достъп;
- извършване на действия и други мерки съгласно ЗМИП, ЗМФТ и актовете по прилагането им.

Минималното съдържание на вътрешни правила за контрол и предотвратяване изпирането на пари и финансирането на тероризма следва да съответства на изискванията на чл. 101, ал. 2 от ЗМИП.

IV. 1. 2. Определяне на лице, което да осъществява вътрешния контрол по изпълнението на задълженията, определени в ЗМИП, ППЗМИП и ЗМФТ

Пощенските оператори и техните представители по чл. 4, т. 7 от ЗМИП могат да създадат специализирани служби по чл. 106 от ЗМИП или да изпълняват лично или чрез лицата, които ги представляват и управляват вътрешния контрол по изпълнението на задълженията си по този закон и правилника за прилагането му. Във втория случай чл. 107 от ЗМИП дава възможност на **управляващите на пощенските оператори и техните представители да делегират задълженията си** чрез определяне на ниво висше ръководство на лице, което да осъществява вътрешния контрол по изпълнението на задълженията, определени в ЗМИП, ППЗМИП и ЗМФТ от този пощенски оператор или представител. Разпоредбите на чл. 106 и чл. 107 от ЗМИП предвиждат задължения за уведомяване на САД ФР – ДАНС.

IV. 1. 3. Обучение

Всички пощенски оператори и техните представители са задължени да осигурят непрекъснато обучение на служителите си, за запознаването им с правилата, свързани с ИП/ФТ или всяко друго сериозно престъпление, свързано с ИП/ФТ, което да ги подпомогне при разпознаването на операции и действия, които могат да бъдат свързани с ИП/ФТ или всяко

друго сериозно престъпление, свързано с ИП/ФТ, а също и с процедурите, които трябва да се спазват в тези случаи.

V. КОМПЛЕКСНА ПРОВЕРКА НА КЛИЕНТА (КПК)

Пощенските оператори и техните представители са длъжни да прилагат мерките за комплексна проверка на клиента, предвидени в Глава втора на ЗМИП.

V. 1. МОМЕНТ НА ИЗВЪРШВАНЕ НА КОМПЛЕКСНАТА ПРОВЕРКА НА КЛИЕНТА

Пощенските оператори и техните представители следва да извършват комплексна проверка на клиентите, които искат да встъпят в делови взаимоотношения с тях или да извършат случайна сделка или операция. Моментът, към който пощенските оператори и техните представители са длъжни да извършват комплексна проверка на клиента са подробно уредени в Глава втора от ЗМИП. Необходимо е да се обърне особено внимание и да се прави разграничение по отношение на момента на извършване на отделните мерки по чл. 10, т. 1 – 5 от ЗМИП.

В случаите, когато мерките за комплексна проверка не могат да бъдат приложени, пощенският оператор или неговият представител е длъжен да откаже извършването на операцията или сделката или установяването на делови взаимоотношения. В случаите на вече установени делови взаимоотношения, той е длъжен да прекрати тези взаимоотношения. В тези случаи пощенският оператор или неговият представител следва да и извърши преценка дали да уведоми дирекция "Финансово разузнаване" на Държавна агенция "Национална сигурност" чрез уведомление за съмнителна сделка/операция/клиент.

V. 2. МЕРКИ ЗА ИЗВЪРШВАНЕ НА КОМПЛЕКСНА ПРОВЕРКА НА КЛИЕНТА

V. 2. 1. Опознаване на клиента – идентификация, действителна собственост, произход на средства и имуществено състояние (богатство), наблюдение

Съгласно чл. 10 от ЗМИП комплексната проверка на клиента включва:

1. идентифициране на клиента и проверка на неговата идентификация въз основа на документи, данни или информация, получени от надеждни и независими източници;
2. идентифициране на действителния собственик (за юридически лица и други правни образувания) и предприемане на подходящи действия за проверка на неговата идентификация по начин, който дава достатъчно основание на лицето по чл. 4, т. 7 да приеме за установен действителния собственик, включително прилагане на подходящи мерки за изясняване на структурата на собственост и контрол на клиента;
3. събиране на информация и оценка на целта и характера на деловите взаимоотношения, които са установени или предстои да бъдат установени с клиента, в предвидените от ЗМИП случаи;
4. изясняване на произхода на средствата, в предвидените от ЗМИП случаи;
5. текущо наблюдение върху установените делови взаимоотношения, задълбочена проверка и анализ на сделките и операциите, извършвани през цялото времетраене на тези

взаимоотношения, за да се установи доколко те съответстват на рисковия профил на клиента и на събраната при прилагане на мерките по т. 1 – 4 информация за клиента и/или за неговата стопанска дейност, както и да поддържат и своевременно да актуализират относимите документи, данни и информация.

Пощенските оператори и техните представители следва да идентифицират физическите лица, юридическите лица и другите правни образувания, както и да идентифицират и проверят идентификацията на действителните собственици и да идентифицират и проверят идентификацията на физическите лица, претендиращи да действат от името и за сметка на клиент. Действията по идентификации и проверка на идентификацията задължително **се документират** с достоверна дата, имена, длъжност и подпис на служителя, извършил идентификацията и проверката ѝ.

По отношение на идентификацията на действителния собственик, следва да се прилагат **Насоките за идентифициране на действителните собственици на юридически лица и други правни образувания**, публикувани на интернет страницата на ДАНС⁴.

В случаите на установени делови взаимоотношения от пощенските оператори и техните представители не се изисква да идентифицират клиент, който вече е представил достатъчно доказателства за самоличността си и данните, които се изискват по закон, освен ако не се съмняват в истинността на получените документи, данни и информация. Събраните документи данни и информация въз основа на вече извършена комплексна проверка на клиента обаче трябва да се актуализират редовно при съобразяване на рисковия профил на клиента.

В случай че е част от група, пощенският оператор или неговият представител може да разчита на трета страна – част от групата, да извършва отделни мерки за комплексна проверка на клиента, въпреки че крайната отговорност за извършването на мерките за комплексна проверка остава при него **и следва да бъдат изпълнени редица, предвидени в ЗМИП условия**.

V. 3. ВИДНИ ПОЛИТИЧЕСКИ ЛИЧНОСТИ (ВПЛ)

По отношение на МИП/МФТ, свързани с видни политически личности, следва да се прилагат **Насоките за идентифициране на видни политически личности, свързаните им лица и установяване на произхода на средствата и източника на богатствата им**, публикувани на интернет страницата на ДАНС⁵.

V. 4. РАЗШИРЕНА КОМПЛЕКСНА ПРОВЕРКА

Пощенският оператор или неговият представител е длъжен винаги да прилага мерки за комплексна проверка на клиентите, но някои ситуации изискват прилагането на мерки за разширена комплексна проверка в случаите и по реда, предвидени в ЗМИП (Глава втора, Раздел IV). Разширената комплексна проверка на клиентите трябва да се прилага за физически и юридически лица, които представляват по-висок риск за пощенските оператори и техните представители.

⁴ https://dans.bg/upload/345/Pr1_Nasoki_dejstvit_sobstvenik_bul.pdf

⁵ https://dans.bg/upload/356/Nasoki_VPL%20%281%29.pdf

Пощенските оператори и техните представители следва да прилагат също мерки за разширена комплексна проверка когато сметат, че рискът от ИП/ФТ е по-висок поради естеството на деловото взаимоотношение, формата и начина на сключване на сделката, бизнес профила на клиента или други обстоятелства, свързани с клиента.

Пощенските оператори и техните представители оп чл. 4, т. 7 от ЗМИП прилагат мерки за разширена комплексна проверка в следните случаи:

(1) при встъпване в делови взаимоотношения с лица по чл. 36 от ЗМИП (видни политически личности) и в хода на такива взаимоотношения, както и при извършване на случайна операция или сделка по чл. 11 – 13 от ЗМИП с видни политически личности;

(2) при встъпване в делови взаимоотношения и в хода на такива взаимоотношения, както и при извършване на случайна операция или сделка с физически лица, юридически лица и други правни образувания, установени във високорискови държави по чл. 46 от ЗМИП, в т.ч. и държави, определени от Групата за финансови действия срещу изпирането на пари (FATF) като високорискови⁶;

(3) при продукти, операции и сделки, които биха могли да доведат до анонимност и по отношение на които не са предвидени допълнителни мерки по ЗМИП;

(4) при нови продукти, бизнес практики и механизми за доставка, когато същите са оценени като високорискови по реда на глава седма;

(5) във връзка с нови технологии при нови или вече съществуващи продукти, бизнес практики и механизми за доставка, когато същите са оценени като високорискови в НОР или в собствената оценка на риска;

(6) при сложни или необичайно големи сделки или операции, при сделки или операции, които се извършват по необичайни схеми, както и при операции и сделки без явна икономическа или законна цел;

(7) във всички други случаи, при които в НОР или в собствената оценка на риска е установен по-висок риск от изпиране на пари или финансиране на тероризъм.

Мерките за разширена комплексна проверка са подробно описани в чл. 37 – 41, 46 – 49 и 51 от ЗМИП и чл. 25 – 33 от ППЗМИП. По отношение на мерките за разширена комплексна проверка приложение намират и включват стратегиите и мерките за ограничване на риска, изброени в Приложение 2.

V. 5. ОПРОСТЕНА КОМПЛЕКСНА ПРОВЕРКА

Мерки за опростена за комплексна проверка са неприложими винаги, когато има съмнение за изпиране на пари или финансиране на тероризъм, когато трябва да се приложи разширена комплексна проверка или когато клиентът или ситуацията са оценени като среден или по-висок риск.

Мерки за опростена комплексна проверка могат да се прилагат само при кумулативното наличие на предвидените в ЗМИП и ППЗМИП условия.

⁶ Държави, за които FATF е публикувала „call for action“.

Мерки за опростена комплексна проверка могат да се прилагат само след като пощенският оператор или неговият представител е уведомил предварително дирекция "Финансово разузнаване" на Държавна агенция "Национална сигурност" за идентифицираните категории клиенти, продукти и услуги с по-нисък риск и за намерението да се прилагат опростени мерки за комплексна проверка спрямо тях.

VI. ТЕКУЩО И РАЗШИРЕНО НАБЛЮДЕНИЕ

VI. 1. ТЕКУЩО НАБЛЮДЕНИЕ

Пощенските оператори и техните представители полагат дължимата грижа при наблюдението на стопанската дейност, извършвана от техните клиенти, като по този начин гарантират познаване на бизнеса на клиента, произхода на средства, предвиденото естество и цел на деловите взаимоотношения, операциите или сделките на клиента. **Не се извършва текущо наблюдение, когато не са установени делови взаимоотношения.**

VI. 2. РАЗШИРЕНО НАБЛЮДЕНИЕ – ВПЛ, ВИСОКОРИСКОВИ ДЪРЖАВИ, ТРАНСГРАНИЧНИ СДЕЛКИ И КЛИЕНТИ

Пощенските оператори и техните представители следва да поставят под текущо и разширено наблюдение деловите си взаимоотношения, операциите и сделките с лица – видни политически личности, както и лица от високорискови трети държави по чл. 46 от ЗМИП, в т.ч. и държави, определени от Групата за финансови действия срещу изпирането на пари (FATF) като високорискови, като повишават броя и честотата на извършваните проверки и идентифицират схеми на сделки и операции, които налагат допълнително проучване.

Пощенските оператори и техните представители трябва да поставят под разширено наблюдение и всички сложни или необичайно големи сделки или операции, всички сделки или операции, които се извършват по необичайни схеми, както и всички сделки и операции, които нямат явна икономическа или законна цел, дори в случаите, в които все още не са открити причини за съмнение за изпиране на пари, финансиране на тероризъм или пролиферация във връзка с такива сделки. Особено внимание следва да се обръща в случаите на сделки и клиенти, чийто обхват надхвърля границите на страната.

Пощенските оператори и техните представители също трябва да анализират основанийето и целта на такива сделки и да документират резултатите от анализа. Те трябва да бъдат достъпни при поискване от САД ФР – ДАНС, надзорните и правоприлагащите органи. Пощенските оператори и техните представители трябва да уведомяват за всички съмнителни сделки.

VII. УВЕДОМЯВАНЕ ЗА СЪМНИТЕЛНИ СДЕЛКИ/ОПЕРАЦИИ/КЛИЕНТИ

Пощенският оператор и неговият представител е длъжен да уведомява САД ФР – ДАНС за съмнителни сделки/операции и клиенти, незабавно след възникване на съмнението (чл. 72 от ЗМИП и чл. 9 от ЗМФТ). Това изискване се прилага както за вече сключени сделки, така и за такива, които са в процес на сключване.

Съгласно чл. 72, ал. 1 от ЗМИП, при съмнение и/или узнаване за изпиране на пари и/или за наличие на средства с престъпен произход Пощенският оператор и неговият представител е

длъжен да уведоми незабавно дирекция "Финансово разузнаване" на Държавна агенция "Национална сигурност" преди извършването на операцията или сделката, като забави нейното осъществяване в рамките на допустимия срок съгласно нормативните актове, уреждащи съответния вид дейност. В уведомлението Пощенският оператор или неговият представител посочва максималния срок, в който операцията или сделката може да се отложи.

Когато забавянето на операцията или сделката, за която Пощенският оператор или неговият представител е уведомил САД ФР – ДАНС, е обективно невъзможно или има вероятност това да осуети действията по преследване на бенефициерите на съмнителна сделка или операция, пощенските оператори и техните представители уведомяват дирекция "Финансово разузнаване" на Държавна агенция "Национална сигурност" незабавно след извършването ѝ, като посочва причините, поради които забавянето е било невъзможно.

Съгласно чл. 9, ал. 3 от ЗМФТ, при съмнение и/или узнаване за финансиране на тероризъм пощенските оператори и техните представители са длъжни да уведомят незабавно и дирекция "Финансово разузнаване" на Държавна агенция "Национална сигурност" преди извършване на операцията или сделката, като забавят нейното осъществяване в рамките на допустимия срок съгласно нормативните актове, уреждащи съответния вид дейност. В уведомлението пощенските оператори и техните представители посочват максималния срок, в който операцията или сделката може да се отложат. В тези случаи дирекцията упражнява правомощията си по чл. 74 и 90 от Закона за мерките срещу изпирането на пари.

Дирекция "Финансово разузнаване" на Държавна агенция "Национална сигурност" може да получи информация за финансиране на тероризъм освен от лицата по чл. 4 от Закона за мерките срещу изпирането на пари, и от техни служители, които не отговарят за прилагането на мерките срещу финансирането на тероризма. В тези случаи дирекцията упражнява правомощията си по чл. 74 и 90 от Закона за мерките срещу изпирането на пари.

В Дирекция „Финансово разузнаване“ на ДАНС е внедрена и функционира автоматизирана информационна система **goAML**, разработена от Службата на ООН по наркотиците и престъпността, която е достъпна за задължени лица по чл. 4 от ЗМИП след регистрация на адрес <https://aml.dans.bg>. На началната страница на системата са налични **Указания за регистрация**⁷. Системата предоставя на регистрираните задължени лица по чл. 4 от ЗМИП възможност да създадат и управляват собствен AML профил, чрез който да автоматизират процеса по подаване на уведомления за съмнителни/сделки/операции/клиенти и уведомления за плащания в брой чрез попълване на онлайн формуляр или чрез утвърдена от директора на Дирекция „Финансово разузнаване“ на ДАНС xml схема. Системата позволява на задължените лица по чл. 4 от ЗМИП да регистрират свои служители, на които да възлагат изпълнението на отделни части от процеса на изготвяне и изпращане на уведомленията.

До момента на цялостно преминаване на подаването на уведомления по чл. 72 и чл. 76 от ЗМИП чрез системата goAML, за нерегистрираните задължени лица на интернет страницата на ДАНС е публикуван образец на уведомление за съмнителна сделка/операция/клиент.

Приложение 3 съдържа примерен списък с критерии за съмнение, който пощенските оператори и техните представители могат да ползват. Разширен примерен списък е достъпен за регистрираните потребители на системата goAML.

⁷ https://dans.bg/upload/3460/goaml_registration_bul%281%29.pdf

Важно е да се има предвид, че срещу пощенският оператор и неговият представител, неговите органи за управление, собственици, служители, съдружници, професионалисти и служители не може да бъде образувано наказателно, гражданско, дисциплинарно или административно производство за нарушаване на банковата или професионалната тайна при добросъвестно подаване на уведомление за съмнителна сделка. На интернет страницата на ДАНС⁸ са публикувани „Указания за уведомяване на дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“ по чл. 72 от Закона за мерките срещу изпирането на пари и чл. 9 от Закона за мерките срещу финансирането на тероризма“. Указанията съдържат изискванията за уведомяване и информация за попълване и подаване на уведомления за съмнителни сделки или операции и клиенти.

В случаите на получени уведомления за съмнения по реда на чл. 72, 88 и 89 от ЗМИП и съответно чл. 9, ал. 3 и 6 от ЗМФТ, САД ФР – ДАНС има правомощия за изискване на информация по реда на чл. 74 от ЗМИП, както е описано в т. XI.2.

VIII. СЪХРАНЯВАНЕ НА ИНФОРМАЦИЯ

VIII. 1. СРОК ЗА СЪХРАНЯВАНЕ НА ИНФОРМАЦИЯ

Пощенските оператори и техните представители съхраняват за срок от 5 години всички събрани и изготвени по реда на ЗМИП и ППЗМИП документи, данни и информация. Конкретните изисквания и началото на срока се съдържат в чл. 67 от ЗМИП. По писмено указание на директора на САД ФР – ДАНС сроковете за съхранение могат да бъдат удължени с до 2 години.

Учредените на територията на Република България юридически лица и други правни образувания, техните управляващи и представляващи, техните ликвидатори, както и физическите лица за контакт по чл. 63, ал. 4, т. 3 от ЗМИП са длъжни да съхраняват точна и актуална информация относно физическите лица, които са техни действителни собственици, включително с подробни данни относно притежаваните от тях права, за срок от **5 години след прекратяването на юридическото лице или друго правно образувание**. Това задължение възниква и за всички лица извън горепосочените, извършващи дейности във връзка с прекратяването на юридическото лице или друго правно образувание.

Физическите и юридическите лица и други правни образувания, които са установени или пребивават на територията на Република България в качеството си на доверителни собственици или лица, заемащи сходни длъжности в тръстове, попечителски фондове и други подобни чуждестранни правни образувания, учредени и съществуващи съобразно правото на юрисдикциите, допускащи такива форми на доверителна собственост, и физическите лица за контакт по чл. 63, ал. 4, т. 3 от ЗМИП са длъжни да съхраняват подходяща, точна и актуална информация относно физическите лица, които са действителни собственици на доверителната собственост за срок от **5 години след прекратяването на тръста, попечителския фонд или друго подобно чуждестранно правно образувание**. Това задължение възниква и за всички лица, извършващи дейности във връзка с прекратяването на тръста, попечителския фонд или друго подобно чуждестранно правно образувание.

⁸ https://dans.bg/upload/3392/ukazaniq_zmip_72_zmft_9-18032024.pdf

Съгласно чл. 68 от ЗМИП документите и информацията следва да се съхраняват така, че да са на разположение на САД ФР – ДАНС, съответните надзорни органи и на одиторите и да се предоставят на дирекция "Финансово разузнаване" на Държавна агенция "Национална сигурност" при поискване в оригинал, служебно заверен препис, извлечение или справка в определения от директора на дирекцията срок и формат.

IX. ЧУЖДЕСТРАННИ КЛОНОВЕ И ДЪЩЕРНИ ДРУЖЕСТВА

IX. 1. ИЗИСКВАНИЯ ЗА ПРИЛАГАНЕ НА МЕРКИТЕ СРЕЩУ ИП/ФТ, ПРИЛОЖИМИ КЪМ ЧУЖДЕСТРАННИ КЛОНОВЕ И ДЪЩЕРНИ ДРУЖЕСТВА

Пощенските оператори и техните представители, които имат чуждестранни клонове и мажоритарно притежавани дъщерни дружества, трябва да изискват прилагане на мерките срещу ИП/ФТ до степента, която националното законодателство позволява.

Когато законодателството на третата държава не позволява прилагането на някои от мерките за предотвратяване на изпирането на пари, финансирането на тероризма и пролиферация в обхвата, предписан от ЗМИП, пощенските оператори и техните представители трябва да информират своя надзорен орган и да предприемат адекватни мерки за премахване на риска от изпиране на пари или финансиране на тероризма.

Пощенските оператори и техните представители трябва редовно да информират чуждестранните клонове и мажоритарно притежаваните дъщерни дружества за вътрешния контрол, свързан с предотвратяването на изпиране на пари, финансиране на тероризма и пролиферация, особено по отношение на комплексна проверка на клиента, предоставяне на данни и информация, съхранение на документи и други значими обстоятелства, свързани с изпиране на пари, финансиране на тероризма и пролиферация.

X. ЦЕЛЕВИ ФИНАНСОВИ САНКЦИИ ЗА ФИНАНСИРАНЕ НА ТЕРОРИЗМА

Пощенските оператори и техните представители следва да следят дали не държат или управляват имущество, за което знаят, че е притежавано или контролирано лично или от името на терорист или терористична група или е свързано с финансиране на тероризъм. Това включва информация за всяка сделка или предложена сделка, свързана с пощенски паричен превод.

При наличие на информация че имущество, което пощенският оператор или неговият представител държи, е притежавано или контролирано лично или от името на включено в съответните списъци лице, до САД ФР – ДАНС трябва незабавно да бъде изпратено уведомление за ФТ. Ако се знае, че сделка е свързана със собственост, притежавана или контролирана лично или от името на включено в съответните списъци лице, тя не трябва да се сключва. В случай на съмнение, че става въпрос за лице от антитерористичните списъци, се изисква подаването на уведомление за съмнителна сделка/клиент до САД ФР – ДАНС, ако сделката е била вече сключена. Уведомлението се подава и ако е направен опит за сключване на съмнителна сделка.

В Закона за мерките срещу финансиране на тероризма (ЗМФТ) са определени мерките срещу финансирането на тероризма, както и редът и контролът за тяхното прилагане. Целите на ЗМФТ са предотвратяване и разкриване на действия на физически лица, юридически лица, групи и организации, насочени към финансиране на тероризма. В чл. 3 на закона са изброени

мерките срещу финансиране на тероризма, а именно: блокиране на финансови средства и други финансови активи или икономически ресурси, и забрана за предоставяне на финансови услуги, финансови средства и други финансови активи или икономически ресурси. Съгласно чл. 4б, тези мерки се прилагат спрямо:

- физически лица, юридически лица, групи и организации, спрямо които са наложени санкции за тероризъм или финансирането му с регламент на Съвета на Европейския съюз;

- физически лица, юридически лица, групи и организации, посочени от Съвета за сигурност на Организацията на обединените нации като свързани с тероризъм или финансирането му или спрямо които са наложени санкции за тероризъм или финансирането му с резолюция на Съвета за сигурност на Организацията на обединените нации – след публикуване на информацията по чл. 5а, ал. 1, т. 2;

- физически лица, юридически лица, групи и организации, включени в списък, приет с решение на Министерския съвет.

Линк към Консолидирания списък с лица, групи и организации, обект на финансови санкции от страна на Европейския съюз, може да бъде намерен на интернет страницата на ДАНС⁹.

Линк към списъка с целеви финансови санкции, свързани с финансирането на тероризма и пролиферация, може да бъде намерен на интернет страницата на ДАНС¹⁰.

Интернет страницата на МВнР¹¹ предоставя възможност за абонамент RSS feed за своевременно уведомяване относно промени в антитерористични списъци.

Освен това от пощенските оператори и техните представители може да се изисква да прилагат разширена комплексна проверка, пропорционална на рисковете, към бизнес взаимоотношения и трансакции с физически и юридически лица (включително финансови институции) от държави, за които това се изисква от FATF¹².

XI. ИСКАНИЯ ЗА ИНФОРМАЦИЯ ОТ САД ФР – ДАНС

Съгласно чл. 32д, ал. 1 от Правилника за прилагане на закона за държавна агенция „Национална сигурност“, Специализираната административна дирекция "Финансово разузнаване", получава, съхранява, проучва, анализира и разкрива информация, получена при условията и по реда на ЗМИП, ЗМФТ и ЗДАНС и упражнява контрол по прилагането на превантивното законодателство срещу изпирането на пари и финансирането на тероризма.

Предвид гореизложеното, САД ФР – ДАНС има както функции по получаване, анализ и разкриване на информация за съмнения за изпиране пари или финансиране на тероризъм, така

⁹ <https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en>

¹⁰

https://dans.bg/upload/298/RESHENIE_265_na_MS_ot_23042003_g_za_priemane_Spisyk_na_fiziceskite_lica_uridiceskite_lica_grupite_i_.pdf

¹¹ <https://www.mfa.bg/bg/ministerstvo/un-sanctions>

¹² <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-February-2023.html>

и функции по упражняване на контрол за спазване на изискванията на ЗМИП, ЗМФТ и актовете по прилагането им.

XI. 1. ИСКАНИЯ ЗА ИНФОРМАЦИЯ ОТ САД ФР – ДАНС ВЪВ ВРЪЗКА С ОСЪЩЕСТВЯВАНЕ НА КОНТРОЛНА ДЕЙНОСТ

Във връзка с контролните функции на САД ФР – ДАНС и съгласно чл. 111 от ЗМИП предоставянето на документи, сведения, справки, извлечения, писмени и устни обяснения за целите на проверките, извършвани от определени от председателя на ДАНС длъжностни лица от състава на САД ФР - ДАНС не може да бъде отказано или ограничено по съображения за служебна, банкова, търговска или професионална тайна или че същата представлява данъчна и осигурителна информация или защитена лична информация. Предоставянето на информация по реда на чл. 111 от ЗМИП не поражда отговорност за нарушаване на други закони или на договори.

В предвидените от ЗМИП и ППЗМИП случаи САД ФР – ДАНС може да изисква предоставянето на статистически данни по въпроси, свързани с ефективността на системите за превенция и предотвратяване на изпирането на пари и/или финансирането на тероризма.

XI. 2. ИСКАНИЯ ЗА ИНФОРМАЦИЯ ОТ САД ФР – ДАНС ПО РЕДА НА ЧЛ. 74 ОТ ЗМИП

Във връзка с функциите на САД ФР - ДАНС по получаване, анализ и разкриване на информация за съмнения за изпиране пари или финансиране на тероризъм, **съгласно чл. 74 от ЗМИП, САД ФР – ДАНС има право да иска от всички задължени субекти по чл. 4 от ЗМИП информация относно съмнителни операции, сделки или клиенти. Предоставянето на информацията не може да бъде отказано или ограничено по съображения за служебна, банкова, търговска или професионална тайна или че същата представлява данъчна и осигурителна информация или защитена лична информация.**

XI. 3. ПРОВЕРКА НА МЯСТО

При осъществяване на контролната си дейност, съгласно ЗМИП контролните органи на САД ФР – ДАНС имат право на свободен достъп в служебните помещения на проверявания субект, за да се извърши проверка на място без предварително уведомление.

След приключване на проверката контролният орган на САД ФР – ДАНС ще обобщи резултатите от проверката устно. Констативен протокол, в който се посочват всички недостатъци, ще бъде предоставен от САД ФР – ДАНС след проверката на място. От пощенския оператор или неговия представител ще бъде поискан и план за действие и ще му бъдат дадени срокове за отстраняване на недостатъците.

XI. 4. САНКЦИИ ЗА НЕСПАЗВАНЕ НА МЕРКИТЕ СРЕЩУ ИЗПИРАНЕТО НА ПАРИ ИЛИ ФИНАНСИРАНЕТО НА ТЕРОРИЗМА

Въпреки че повечето задължени по ЗМИП лица се стремят да спазват изискванията на ЗМИП, ППЗМИП и ЗМФТ, неизменно някои имат пропуски, а други не се съобразят изцяло или отчасти. ЗМИП предвижда административни наказания, които се налагат за неспазване на предвидените в него задължения на субектите по чл. 4 от него. **Глобите и имуществените санкции варират от 1000 лв. до 10 000 000 лв. или до 10 на сто от годишния оборот, в зависимост от тежестта на нарушението.**

Чл. 123а, ал. 2 от ЗМИП определя за кои нарушения на ЗМИП и ЗМФТ не се прилагат правилата за маловажност.

Глава 8 от ППЗМИП урежда реда за определяне на размерите на глобите и имуществените санкции, налагани за нарушения на разпоредбите на ЗМИП.

За да разберете по-добре обхвата на потенциалните нарушения и наказания, се препоръчва запознаване с Глава 10 от ЗМИП, чл. 15 и 16 от ЗМФТ, и Глава 8 от ППЗМИП.

XII. ЗАКЛЮЧЕНИЕ

Пощенските оператори и техните представители се насърчават да прилагат насоките, предоставени с този документ, за да се предпазят от ИП/ФТ, но също така и за да гарантират добрата репутация на своята професия.

ПРИЛОЖЕНИЕ 1– Рискове, свързани с клиента, предлаганите услуги и географски риск за пощенските оператори и техните представители

В настоящото приложение са изброени неизчерпателно някои от най-често срещаните фактори/индикатори, които да подпомогнат оценката на риска при пощенските парични преводи (в т.ч. и наложен платеж). Настоящото приложение следва да се използва заедно с **Насоките за изготвяне на оценка на риска от изпиране на пари и финансиране на тероризма**, публикувани на интернет страницата на ДАНС.

Географски фактори

- При идентифициране на рисковете, свързани с географски райони и други държави, включително произхода на юридически лица, както и на физически лица, пощенските оператори трябва да определят дали е налице висок риск, като вземат предвид следните географски фактори:

- Ефективността на правния режим на съответната държава за борба с изпирането на пари/финансирането на тероризъм и дали е установено, че има недостатъци.
- Нивото и естеството както на заплахите, така и на уязвимостите, свързани с пощенските парични преводи в дадената географска област.
- Нивото на правна прозрачност и съответствие със съществуващите правни режими за държави, за които е установено, че им липсват ефективни закони и разпоредби за борба с изпирането на пари/финансирането на тероризма.
- Дали дадена държава е обект на санкции, ембарго или подобни мерки, издадени от международни организации като ООН.
- Дали средствата са генерирани от чужбина и бизнес отношенията са били водени без срещи лице в лице

Риск, свързан с клиента

-
- Встъпването в делово взаимоотношение и по-нататъшното развитие на същото се осъществяват по такъв начин, който е позволил непоследователност в поведението на клиентите, избягване на контакт лице в лице в необичайни ситуации.
 - Извършване на множество последователни/ или през недълъг период сделки с малка стойност.
 - Ненужно налягане или необичайно бързано от страна на клиента, за да бъде осъществена услугата бързо.
 - Използване на различни документи за самоличност от едно и също лице.
 - Наличие на необичайни преводи към ЮЛНЦ.
 - Ако за клиента, действителния собственик или някакви свързани с тях лица, има публично достъпна информация, че са тясно свързани с дейности по ИП/ФТ, или са осъдени или заподозрени, че са съучастници в такива дейности.
 - Клиентът или действителния собственик има политически връзки и се счита за ВПЛ или клиентът или действителния собственик има други връзки с ВПЛ или лица, които заемат видна политическа или обществена позиция.

Рискове, свързани със сделката

- Използването на трети лица, за изпращане или получаване на средства.
- Необясними или внезапни промени във финансовите възможности на клиента.
- Използване на пари в брой при бърза продажба, размяна на пари директно между продавач и купувач, за включване на паричен депозит или голяма еднократна парична транзакция.
 - Разходите по сделката или фактурите на продавача или купувача се плащат от трета страна, която няма връзка със сделката, или чрез необичайни канали (напр. несвързана финансова институция).
 - Искания за ускоряване на сключването на сделки, евентуално над или под дадена стойност.
 - Изпращане/ получаване на парични средства в/ от във високорискова юрисдикция;
 - Наложено плащане на трета страна, очевидно несвързана с транзакцията.

ПРИЛОЖЕНИЕ 2 – Мерки за ограничаване на риска

Мерките за ограничаване на риска за ситуации с висок риск могат да включват:

- повишена информираност за ситуации с по-висок риск в рамките на делови взаимоотношения в цялото предприятие;
- повишено наблюдение на сделките;
- получаване на одобрение за встъпване в делово взаимоотношение от висшето ръководство;
- повишаване на нивата на текущите контроли и наблюдение на деловите взаимоотношения;
- персонал, който има ясни задачи, отговорност и отчетност;
- адекватно разпределение на задълженията (например служител, установяващ връзка с клиент, няма власт да го одобри, тъй като това разрешение е отговорност на някой друг в организацията);
- правилни процедури за разрешение (например служител, обработващ сделка, за която сумата надвишава определен праг, трябва да спазва процедура, за да получи одобрение за сделката от някой друг в организацията);
- вътрешни прегледи за правилно определяне на оценката на риска;
- търсене на допълнителна информация извън минималните изисквания за установяване на самоличността на клиента или действителния собственик на клиент юридическо лице или друго правно образувание;
- получаване на допълнителна информация за предвиденото естество на сделката, включително оценки относно размера и вида на бизнес дейността;
- получаване на допълнителна информация относно произхода на средства на клиента и източника на имуществено състояние и нейното документиране;
- изискване от високорискови клиенти да предоставят допълнителна, документална информация относно контролите, които са внедрили, за да защитят своите сделки от използването им за целите на ИП/ФТ;
- извършване на независима проверка на информацията (т.е. от надежден източник, различен от клиента);
- спиране на всяка сделка с потенциален клиент, докато не бъде получена информация за идентификация;
- прилагане на подходящ процес за одобряване на всички взаимоотношения, идентифицирани като високорискови, като част от процеса на приемане на клиента или отказ от встъпване в делови взаимоотношения с потенциални клиенти, тъй като те превишават нивото на толерантност към риска;
- въвеждане на процес за прекратяване на високорисково делово взаимоотношение, което е извън заявеното ниво на толерантност на риска;
- анализиране на уязвимостите за изпиране на пари и финансиране на тероризъм при нови начини за придобиване и при разработване на продукти или услуги.

ПРИЛОЖЕНИЕ 3 - примерен списък с критерии за съмнение, който пощенските оператори и техните представители могат да ползват.

1. Наличие на негативна информация в открити източници за водени разследвания, досъдебни производство или друг вид престъпна дейност по отношение на страна по сделката.
2. Клиентът се държи агресивно, настоятелно, колебливо, или видимо не е запознат с естеството на извършваната от него операция или се опитва да прикрие произхода на средствата, с които същата се извършва.
3. Клиентът се придружава от трето лице, което взема крайните решения.
4. Видима незаинтересованост от страна на клиента по отношение на условията, таксите и комисионните по извършваната операция.
5. Демонстриране на прекалена заинтересованост и/или познания от страна на клиента за законодателството и вътрешно нормативните актове за мерки срещу ИП/ФТ, с цел тяхното заобикаляне.
6. Страна по операцията фигурира в санкционни списъци на Министерски съвет, ЕС, ООН, Министерство на финансите на САЩ или на други държави.
7. Страна по операцията се свързва с държава, категоризирана като конфликтна зона или граничеща с такава, или по отношение на същата е налична информация за подкрепа на терористични дейности.
8. Страна по операцията се свързва с държава, която е известна с производство и/или разпространение на наркотици, трафик на хора и нелегална миграция.
9. ВПЛ се стреми към прекомерна поверителност, предоставя неточна или непълна информация, която не може да бъде проверена.
10. Изпращане на множество преводи за малки суми, в т.ч и преводи с банкноти в малки купюри, от едно лице към множество различни лица.
11. Парични преводи с висока честота, получавани в рамките на кратък период от време (няколко дни), чиито общ размер е значителен.
12. Предаване на съмнителни пощенски пратки.
13. Трансфери от представители на юридически лица или дарителски организации към дружества, регистрирани в конфликтна зона или граничеща с такава, или по отношение на същата е налична информация за подкрепа на терористични дейности.
14. Страна по операцията е лице, което е резидент в т.нар. зона с преференциален данъчен режим.
15. Получаване/изпращане на средства в няколко различни офиса в различни локации, и/или ползване на различни документи за самоличност от едно лице.
16. Получаване/изпращане на средства от лица, предоставящи един и същ документ за самоличност.

17. Индикации за умишлено раздробяване на сумите и извършване на няколко по-малки по размер операции, включително и когато същите са под законово определен праг, свързан с прилагане на мерки за комплексна проверка.

18. Липса на видима връзка между страните по извършваната операция.

19. Клиентът използва документи за самоличност, чиято валидност/истинност трудно може да бъде проверена.

20. Получаване на преводи с висока честота, с незабавно трансфериране на средствата в полза на трето лице.

21. Изпращане на преводи от множество лица в полза на едно лице и обратно.

22. Получаване/изпращане на преводи от лице със съмнителен профил, който не предполага извършване на операции в такъв мащаб.

23. Наличие на информация, че операцията вероятно е свързана с измама.

24. Използване на услугите на пощенски оператор, въпреки наличието на по-логични алтернативи за осъществяване на операцията.

25. Получаване/изпращане на преводи под формата на дарения в голям размер от НПО в полза на физическо лице или обратното.

ПРИЛОЖЕНИЕ 4 - Списък с методически указания, насоки и друга полезна информация

1. **УКАЗАНИЯ** за регистрация на лица по чл. 4 от Закона за мерките срещу изпирането на пари (ЗМИП) в системата goAML за автоматизирано подаване на уведомления за съмнителни сделки/операции/клиенти към дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“ и предоставяне на друга информация по ЗМИП и Закона за мерките срещу финансирането на тероризма (ЗМФТ)
2. **НАСОКИ** за изготвяне на оценка на риска от изпиране на пари и финансиране на тероризъм
3. **НАСОКИ** за идентифициране на действителни собственици на юридически лица и други правни образувания. Рискови фактори, относими към юридически лица, съгласно Националната оценка на риска от ИП/ФТ. Примерни критерии за съмнение относно опити за прикриване на действителна собственост
4. **Списък на длъжностите**, свързани с изпълнението на важни обществени функции по чл.36, ал.2 от ЗМИП
5. **НАСОКИ** за организацията и дейността на специализираните служби по ЗМИП
6. **НАСОКИ** за идентифициране и проверка на идентификацията на клиенти физически лица (вкл. представляващи, пълномощници и действителни собственици)
7. **УКАЗАНИЯ** за реда за определяне на физическите лица, които подлежат на идентификация като действителни собственици на юридическите лица с нестопанска цел (ЮЛНЦ), регистрирани по Закона за юридическите лица с нестопанска цел (ЗЮЛНЦ)
8. **НАСОКИ** за установяване и идентифициране на видни политически личности, свързаните им лица и специалните изисквания за комплексна проверка по отношение на тази категория лица
9. **РИСКОВИ ИНДИКАТОРИ** за съмнения за изпиране на пари от видни политически личности (ВПЛ)
10. **НАРЪЧНИК** за прилагане на мерките по ЗМИП и ППЗМИП за предотвратяване на злоупотребите с нови технологии, продукти и сделки, които биха могли да доведат до анонимност
11. **НАСОКИ** за установяване и докладване на съмнителни операции/сделки/клиенти по ЗМИП, които биха могли да бъдат свързани с нередности и измами със средства на ЕС
12. **НАСОКИ** за системите за наблюдение, включително разширено наблюдение и проверка на произхода на средствата и източника на имуществено състояние на клиентите, както и презгранични операции и чуждестранни клиенти
13. **РИСКОВИ ИНДИКАТОРИ** за изпиране на пари чрез търговска дейност и други форми на злоупотреба с юридически лица и други правни образувания за целите на изпиране на пари
14. **УКАЗАНИЯ** за уведомяване на дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“ по чл. 72 от Закона за мерките срещу изпирането на пари и чл. 9 от Закона за мерките срещу финансирането на тероризма
15. **УКАЗАНИЯ** за изготвяне на План за въвеждащо и продължаващо обучение на служителите, съгл. чл. 67, ал.1 от ППЗМИП

16. [УКАЗАНИЯ](#) за заявяване за вписване на информация и данни за физически лица, които се считат за действителни собственици на юридическите лица с нестопанска цел, в регистъра на юридическите лица с нестопанска цел при Агенция по вписванията
17. [УКАЗАНИЯ](#) относно приложимостта на регламентираните в чл. 63 от ЗМИП изключения от задължението за вписване на данни за действителни собственици и за приложимостта на чл. 63 от ЗМИП спрямо физическите лица за контакт по чл. 63, ал. 4, т. 3 от ЗМИП
18. [УКАЗАНИЯ](#) относно ефективното управление и намаляване на рисковете, свързани с доставчици и услуги за виртуални активи
20. [УКАЗАНИЯ](#) за прилагане на мерки за противодействие и превенция на финансирането на тероризъм
21. [ПРИМЕРНИ КРИТЕРИИ](#) за разпознаване на съмнителни клиенти, сделки и операции, насочени към финансиране на тероризъм
22. [УКАЗАНИЯ](#) за докладване по Закона за мерките срещу изпирането на пари (ЗМИП) и Закона за мерките срещу финансирането на тероризма (ЗМФТ)
23. [Консолидиран списък с лица, групи и организации, обект на финансови санкции от страна на Европейския съюз](#)
24. [Санкционна политика на Европейския съюз](#)
25. [Санкции на Съвета за сигурност на ООН](#)
26. [Санкции на Министерството на финансите на САЩ - Office of Foreign Assets Control \(OFAC\) - SDN list](#)
27. [Консолидиран списък](#) на лица във връзка със ЗМФТ
28. [ЛИНК](#) към интернет страницата на МВНР относно регистрацията за получаване на най-актуална информация за изменения в санкционните списъци на ООН по отношение на финансиране на тероризъм и пролиферация