

ALLEGATO F AL PTPC 2021 - 2023

PROCEDURA PER LE COMUNICAZIONI DI OPERAZIONI SOSPETTE DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO

Redatto: A. Lino 18.12.2019

Verificato: F. Dellepiane 20.12.2019

Approvato: E. Castanini 24.01.2020
P. Piccini 24.01.2020

Versione: 01

Distribuito: Liguria Digitale S.p.A.

DATI DI CONTROLLO DEL DOCUMENTO

Storia del documento				
versione	data	capitolo/paragrafo	modifica apportata	motivo modifica
01	24.01.2020	---	nessuna	---

Riferimenti a documenti aziendali:

- Piano Triennale per la Prevenzione della Corruzione e della Trasparenza adottato, aggiornato e pubblicato in osservanza alla Legge n. 90/2012 e s.m.i.
- Codice Etico

Riferimenti esterni:

- D.lgs. 22 giugno 2007, n. 109, "Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE" e s.m.i.
- D.lgs. 21 novembre 2007, n. 231, "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" e s.m.i..
- D.M. del Ministero dell'Interno, 25 settembre 2015, "Determinazione degli indicatori di anomalia al fine di agevolare l'individuazione delle operazioni sospette di riciclaggio e di finanziamento del terrorismo da parte degli uffici della pubblica amministrazione".
- Provvedimento della Banca d'Italia - UIF, 4 maggio 2011, "Istruzioni sui dati e le informazioni da inserire nelle segnalazioni di operazioni sospette".
- Provvedimento della Banca d'Italia - UIF, 23 aprile 2018, "Istruzioni sulle comunicazioni di dati e informazioni concernenti le operazioni sospette da parte degli uffici delle pubbliche amministrazioni".

Moduli utilizzati:

- "MODELLO DI TRASMISSIONE al Gestore di informazioni, dati e documenti in relazione a operazioni sospette ai sensi dell'art. 10, comma 4, del d.lgs. n. 231/2007 e dell'art. 7 delle "Disposizioni e procedure interne in materia di comunicazione di operazioni sospette di riciclaggio e di finanziamento del terrorismo".

INDICE

	Pag.
1. INTRODUZIONE	4
1.1. Premessa	4
1.2. Scopo	5
1.3. Area di applicazione	5
1.4. Definizioni e acronimi.....	5
2. DESCRIZIONE DELLA PROCEDURA	8
2.1. Attivazione.....	8
2.2. Input e Output.....	8
2.3. Passi procedurali	9
 3. DISPOSIZIONI FINALI	 12

1. INTRODUZIONE

1.1. Premessa

Con l'entrata in vigore del decreto legislativo 25 maggio 2017, n. 90, che ha recepito la quarta Direttiva Antiriciclaggio (Direttiva UE/2015/849) modificando il decreto legislativo 21 novembre 2007, n. 231, la Pubblica Amministrazione in senso ampio, comprese le società dalla stessa controllate, ha assunto un ruolo primario e attivo nella lotta contro il riciclaggio e il finanziamento del terrorismo.

L'art. 10 del d.lgs. 231/2007 ha, infatti, esteso alcuni degli obblighi previsti per gli altri destinatari della normativa antiriciclaggio, anche agli Uffici delle Pubbliche Amministrazioni responsabili dei seguenti procedimenti amministrativi:

- autorizzazioni e concessioni;
- affidamento di lavori, forniture e servizi;
- sovvenzioni, contributi, sussidi, ausili finanziari e vantaggi economici

Liguria Digitale S.p.a. a norma dell'art. 4, comma 2, del D.lgs. n. 175/2016 come recepito dall'art. 4, comma 3, dello Statuto, ha come oggetto sociale "servizi di committenza a norma dell'art. 11 della L.R. n. 42/2006 e quale articolazione funzionale per l'acquisizione di beni e servizi ICT della Stazione Unica Appaltante di Regione Liguria ai sensi dell'art. 18 della L.R. n. 41/2014". Ne consegue, quindi, che Liguria Digitale S.p.a. è responsabile del procedimento amministrativo di "affidamento di lavori, forniture e servizi" assume le responsabilità connesse ai fini della prevenzione del riciclaggio e del finanziamento del terrorismo .

Per "riciclaggio", a norma dell'art. 2, comma 4, del D.Lgs. 231/2007, si intende:

- la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni;
- l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
- l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
- la partecipazione ad uno degli atti di cui alle lettere a), b) e c), l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione.

Il riciclaggio è considerato tale anche se le attività che hanno generato i beni da riciclare si sono svolte nel territorio di un altro Stato.

Per “finanziamento del terrorismo”, a norma dell’art. 1, comma 1 lett. d) del d.lgs. 109/2007 e dell’art. 2, comma 6, del D.lgs. 231/2007, si intende qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all’intermediazione, al deposito, alla custodia o all’erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali, ciò indipendentemente dall’effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette.

1.2. Scopo

Al fine di favorire l’emersione di fenomeni di riciclaggio e di finanziamento del terrorismo, l’art. 10, comma 4, del d.lgs. 231/2007 prevede che le Pubbliche Amministrazioni e le Società dalle stesse controllate siano tenute a comunicare all’Unità di Informazione Finanziaria, istituita presso la Banca d'Italia, i dati e le informazioni concernenti le operazioni sospette di cui vengano a conoscenza nell’esercizio della propria attività istituzionale.

La presente procedura, in osservanza alla normativa in materia “prevenzione dell’utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo”, è volta a garantire nel contesto organizzativo di Liguria Digitale S.p.A.

- l’efficacia nella rilevazione di operazioni sospette,
- la tempestività della segnalazione alla UIF,
- la riservatezza dei soggetti coinvolti nell’effettuazione della segnalazione
- l’omogeneità dei comportamenti.

1.3. Area di applicazione

La procedura è applicata da tutte le strutture aziendali nello svolgimento delle proprie attività lavorative e, prioritariamente, nell’ambito dei procedimenti amministrativi di “affidamento di lavori, forniture e servizi”.

1.4. Definizioni e acronimi

Nel documento sono utilizzati i seguenti acronimi e/o abbreviazioni:

- “*indicatori di anomalia*”: fattispecie rappresentative di operatività ovvero di comportamenti anomali, finalizzate ad agevolare la valutazione, da parte dei segnalanti, degli eventuali profili di sospetto di riciclaggio o di finanziamento del terrorismo;

-
- *“mezzi di pagamento”*: il denaro contante, gli assegni bancari e postali, gli assegni circolari e gli altri assegni a essi assimilabili o equiparabili, i vaglia postali, gli ordini di accredito o di pagamento, le carte di credito e le altre carte di pagamento, le polizze assicurative trasferibili, le polizze di pegno e ogni altro strumento a disposizione che permetta di trasferire, movimentare o acquisire, anche per via telematica, fondi, valori o disponibilità finanziarie;
 - *“operazione”*: l'attività consistente nella movimentazione, nel trasferimento o nella trasmissione di mezzi di pagamento o nel compimento di atti negoziali a contenuto patrimoniale; costituisce operazione anche la stipulazione di un atto negoziale, a contenuto patrimoniale, rientrante nell'esercizio dell'attività professionale o commerciale;
 - *“operazione sospetta”*: l'operazione che per caratteristiche, entità, natura, collegamento o frazionamento o per qualsivoglia altra circostanza conosciuta in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi a disposizione, acquisiti nell'ambito dell'attività svolta, induce a sapere, sospettare o ad avere motivo ragionevole per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa;
 - *“segnalazione operazione sospetta” (SOS)*: comunicazione delle “operazioni sospette” effettuata dal Gestore delle Segnalazioni Antiriciclaggio alla Unità di Informazione Finanziaria per l'Italia;
 - *“Gestore delle Segnalazioni Antiriciclaggio” (Gestore)* è il Soggetto delegato da ciascuna Pubblica Amministrazione alla valutazione e trasmissione delle SOS alla UIF nella piena osservanza delle disposizioni normative e sulla base delle Linee Guida definite dal Comitato di sicurezza finanziaria, delle Istruzioni sulle comunicazioni di dati e informazioni concernenti le operazioni sospette adottate dalla UIF il 23 aprile 2018 e degli atti conseguenti/correlati;
 - *“UIF”*: l'Unità di Informazione Finanziaria per l'Italia, istituita presso la Banca d'Italia, cioè la struttura nazionale incaricata di ricevere dai soggetti obbligati, di richiedere ai medesimi, di analizzare e di comunicare alle autorità competenti le informazioni che riguardano ipotesi di riciclaggio o di finanziamento del terrorismo; le funzioni e competenze della UIF sono descritte all'art. 6, comma 4, del d.lgs. 231/2007;
 - *“Comitato di sicurezza finanziaria”*: il Comitato di sicurezza finanziaria istituito, con decreto- legge 12 ottobre 2001, n. 369, convertito, con modificazioni, dalla legge 14 dicembre 2001, n. 431, e disciplinato con il decreto legislativo 22 giugno 2007, n. 109, in ottemperanza agli obblighi internazionali assunti dall'Italia nella strategia di contrasto al riciclaggio, al finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa ed

all'attività di Paesi che minacciano la pace e la sicurezza internazionale, anche al fine di dare attuazione alle misure di congelamento disposte dalle Nazioni unite e dall'Unione europea.

2. DESCRIZIONE DELLA PROCEDURA

2.1. Attivazione

La presente procedura si attiva qualora emergano, prioritariamente nell'ambito di tutto il ciclo del procedimento amministrativo di affidamento di forniture e servizi a norma del D.lgs. n. 50/2016 (dalla progettazione, all'affidamento/aggiudicazione, alla sottoscrizione/esecuzione e chiusura del contratto) di competenza di Liguria Digitale S.p.a., operazioni sospette di rilevanza economica, connesse con la trasmissione o la movimentazione di mezzi di pagamento e/o con la realizzazione di obiettivi di natura finanziaria o patrimoniale.

Il sospetto è desunto:

- a) dalle caratteristiche, entità, natura dell'operazione o da qualsivoglia altra circostanza conosciuta da personale di Liguria Digitale S.p.A. in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita;
- b) attraverso l'ausilio di indicatori di anomalia definiti dalla UIF (**Allegato 1**) che:
 - rappresentano una elencazione a carattere esemplificativo di connotazioni di operatività ovvero di comportamenti da ritenere "anomali" e potenzialmente caratterizzanti intenti di riciclaggio o di finanziamento del terrorismo;
 - sono volti a ridurre i margini di incertezza connessi con valutazioni soggettive e di contribuire al corretto e omogeneo adempimento degli obblighi di segnalazione.Tali indicatori di anomalia possono essere dalla UIF integrati, aggiornati o modificati periodicamente, occorrendo pertanto riferirsi costantemente al documento procedurale da ultimo pubblicato

2.2. Input e Output

Le informazioni che entrano in input alla procedura nei vari passi sono

- dati e informazioni afferenti a:
 - l'identità o il comportamento dell'Operatore Economico al quale si riferisce l'operazione;
 - le modalità di richiesta o di esecuzione delle operazioni stesse;

Le informazioni che escono quali output della procedura nei vari passi sono

- "MODELLO DI TRASMISSIONE al Gestore di informazioni, dati e documenti in relazione a operazioni sospette ai sensi dell'art. 10, comma 4, del d.lgs. n. 231/2007 e dell'art. 7 delle "Disposizioni e procedure interne in materia di comunicazione di operazioni sospette di riciclaggio e di finanziamento del terrorismo" (**allegato 2**);
- Segnalazione di Operazione Sospetta da parte del Gestore alla UIF.

2.3. Passi procedurali

2.3.1 Individuazione dei Referenti Unità Organizzativa

I Dirigenti o Quadri apicali a riporto gerarchico diretto al Direttore Generale di Liguria Digitale sono Referenti di 1° livello del Gestore e possono, in relazione alla dimensione e alle attività prestate dall'Unità Organizzativa alla quale sono preposti, individuare per iscritto uno o più Referenti di 2° livello.

Il nominativo dei Referenti di 2° livello deve essere comunicato al Gestore.

2.3.2 Raccolta e prima istruttoria delle informazioni e dati relative a operazioni sospette

Il Referente di 1° o 2° livello:

- a) rileva direttamente nell'ambito della propria attività lavorativa ovvero riceve e raccoglie le segnalazioni, informazioni e dati relative a operazioni sospette ai sensi dell'art. 10, comma 4, del d.lgs. n. 231/2007, provenienti dai dipendenti operanti nell'Unità Organizzativa di riferimento;
- b) effettua tempestivamente una prima istruttoria basata su una valutazione degli elementi oggettivi e soggettivi a disposizione del dipendente, di quelli acquisiti in relazione alle attività da svolgersi da parte del medesimo nonché di quelli connessi immediatamente acquisibili dal Referente e che lo stesso ha ritenuto necessario assumere, coerentemente con la definizione di "operazione sospetta" di cui all'art. 1.4 delle presenti disposizioni.

L'istruttoria è effettuata per l'intera durata della relazione con il soggetto cui si riferisce l'operazione e comprende anche eventuali operazioni rifiutate o interrotte ovvero eseguite in tutto o in parte presso soggetti diversi da Liguria Digitale destinatari di autonomi obblighi di segnalazione.

Ai fini della valutazione si tiene in considerazione

- gli "indicatori di anomalia" di cui all'Allegato 1 alla presente procedura che, seppur costituiscono una elencazione esemplificativa e non esaustiva (anche in considerazione della continua evoluzione delle modalità di svolgimento delle operazioni), riducono i margini di incertezza delle valutazioni soggettive;
- ogni ulteriore comportamento e caratteristica dell'operazione che, sebbene non descritta negli indicatori, sia ritenuta sintomatica di profili di sospetto (ad esempio: incoerenza dell'operazione con l'attività o il profilo economico-patrimoniale del soggetto cui è riferita l'operazione; assenza di giustificazione economica; illogicità, inusualità ed elevata complessità dell'attività che la rendono non vantaggiosa);

2.3.3 Invio al Gestore delle informazioni e dati relative a operazioni sospette

Qualora l'istruttoria evidenzii profili motivati di sospetto, il Referente che ha curato

l'istruttoria compila il "MODELLO DI TRASMISSIONE al Gestore di informazioni, dati e documenti in relazione a operazioni sospette ai sensi dell'art. 10, comma 4, del d.lgs. n. 231/2007 e dell'art. 7 delle "Disposizioni e procedure interne in materia di comunicazione di operazioni sospette di riciclaggio e di finanziamento del terrorismo".

L'invio del "MODELLO" al Gestore è di esclusiva competenza del Referente di 1° livello che è tenuto, preventivamente all'invio e senza ritardo, a verificare la completezza dello stesso e della documentazione da accludere ai fini della descrizione dell'operatività sospetta.

Il flusso informativo è gestito attraverso e-mail. Il Referente di 1° livello provvederà alla trasmissione dal suo indirizzo di posta elettronica aziendale a quello dedicato sos@liguriadigitale.it.

2.3.4 Verifica del Gestore e segnalazione alla UIF

Il Gestore, ricevuto il Modello all'indirizzo e-mail dedicato sos@liguriadigitale.it, procede all'istruttoria finale acquisendo, ove necessario, informazioni e documenti ulteriori attraverso lo stesso Referente di 1° livello, le Unità Organizzative competenti, gli Organi di Controllo aziendali ovvero attraverso Banche Dati a sua disposizione.

Il Gestore, qualora in esito all'istruttoria ritenga sussistere gli elementi qualificanti una "operazione sospetta" come definiti all'art. 1.4 che precede, effettua alla UIF la segnalazione di cui all'art. 10, comma 4, del d.lgs. n. 231/2007 a prescindere dalla rilevanza e dall'importo dell'operazione stessa.

Le segnalazioni alla UIF sono effettuate senza ritardo dal Gestore in via telematica, tramite il portale INFOSTAT-UIF della Banca d'Italia al quale lo stesso deve accreditarsi.

Il contenuto della segnalazione alla UIF si articola in:

- dati identificativi della segnalazione, in cui sono riportate le informazioni che identificano e qualificano la segnalazione;
- elementi informativi, in forma strutturata, sulle operazioni, sui soggetti, sui rapporti e sui legami intercorrenti tra gli stessi;
- elementi descrittivi, in forma libera, sull'operatività segnalata e sui motivi del sospetto;
- eventuali documenti allegati.

Tali elementi sono previsti e descritti in modo dettagliato nel Capo II del provvedimento UIF del 23 aprile 2018 "*Istruzioni sulle comunicazioni di dati e informazioni concernenti le operazioni sospette da parte degli uffici delle pubbliche amministrazioni*"; tali istruzioni potranno essere integrate, aggiornate o modificate dalla UIF occorrendo pertanto riferirsi ai provvedimenti da ultimo assunti pubblicati dalla stessa.

Il Gestore avvisa tempestivamente dell'avvenuta segnalazione alla UIF il Referente di 1° livello e archivia il fascicolo a norma dell'articolo che segue.

2.3.5 Archiviazione

Il Gestore assicura la corretta archiviazione e conservazione, in apposite cartelle di rete secondo sistemi di sicurezza e riservatezza rafforzati, delle comunicazioni ricevute dai Referenti di 1° livello, dell'istruttoria da lui effettuata e delle eventuali segnalazioni di operazione sospetta alla UIF.

L'archiviazione e la conservazione è assicurata anche per le comunicazioni ricevute dai Referenti di 1° livello alle quali non segue alcuna segnalazione di operazione sospetta alla UIF.

La segnalazione di operazione sospetta alla UIF è un atto distinto rispetto alle denunce o comunicazioni di fatti penalmente rilevanti all'Autorità giudiziaria e deve essere effettuata indipendentemente da queste.

La UIF, la Guardia di Finanza e la Direzione Investigativa Antimafia possono comunque richiedere ulteriori informazioni ai fini dell'analisi o dell'approfondimento investigativo della segnalazione al Gestore e all'Ente.

3. DISPOSIZIONI FINALI

3.1. Formazione

Liguria Digitale nel quadro dei programmi di formazione continua del personale adotta misure di adeguata formazione del personale ai fini di assicurare il riconoscimento delle fattispecie meritevoli di essere comunicate alla UIF, tenendo conto dell'evoluzione della normativa in materia.

Fuori dai casi previsti dal D.Lgs. 231/2007 e dalle presenti disposizioni, è fatto divieto di portare a conoscenza di terzi l'avvenuta comunicazione alla UIF o informarli di approfondimenti in corso o effettuati circa operazioni sospette di riciclaggio e di finanziamento del terrorismo.

3.2. Efficacia

Le presenti disposizioni costituiscono parte integrante e sostanziale del Piano Triennale della Prevenzione della Corruzione e sono approvate unitamente al suddetto Piano con la determinazione dell'Amministratore Unico.

Il Gestore, per quanto di competenza, può emanare ulteriori disposizioni attuative e interpretative della presente disciplina.