GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 6124534]

Parere su uno schema di decreto legislativo volto ad attuare la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo - 9 marzo 2017

Registro dei provvedimenti
n. 125 del 9 marzo 2017

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere del Ministero dell'Economia e delle Finanze;

Visto l'art. 154, comma 4, del d.lgs. 30 giugno 2003, n. 196 recante Codice in materia di protezione dei dati personali (di seguito Codice);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

PREMESSO

Il Ministero dell'Economia e delle Finanze ha trasmesso all'Autorità per l'esame uno schema di decreto legislativo volto ad attuare la direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo.

Lo schema di decreto in esame introduce significative modifiche alla vigente disciplina in materia di prevenzione dell'uso del sistema finanziario a fini di riciclaggio e di finanziamento del terrorismo, al fine di allineare la normativa nazionale alle più recenti disposizioni introdotte in materia con la direttiva del Parlamento europeo e del Consiglio, del 20 maggio 2015, (UE) 2015/849 (la quarta del settore), che integra ed abroga le direttive 2005/60/CE e 2006/70/CE e applica le raccomandazioni GAFI.

La direttiva intende operare un più rigoroso contrasto alla crescente diversificazione del mercato criminale, atteso che i flussi di denaro illecito, compromettendo la stabilità e l'integrità del settore finanziario, rappresentano una concreta minaccia per il mercato interno dell'Unione e dei singoli Stati membri. Considerata la natura mutevole delle minacce costituite dal riciclaggio e dal finanziamento del terrorismo, facilitata dalla continua evoluzione della tecnologia e dei mezzi a disposizione dei criminali, l'adozione di misure di contrasto che consentano di adeguare il sistema di prevenzione a nuove ipotesi di riciclaggio è vista come imprescindibile.

Da ciò discende, come indicato nella relazione illustrativa, l'esigenza di un intervento d'insieme volto a migliorare l'aderenza del quadro normativo nazionale alla nuova disciplina comunitaria, nonché a correggere incongruenze, a chiarire dubbi interpretativi e a rimuovere le difficoltà emerse nel corso degli anni, in sede di applicazione del d.lgs. 21 novembre 2007, n.231, al fine di rendere la disciplina funzionale al migliore assolvimento dei compiti imposti dal legislatore europeo.
Il potere di modifica della normativa antiriciclaggio è espressamente previsto dall'articolo 15 della legge 12 agosto 2016, n. 170 (c.d. "legge di delegazione europea 2015").

RILEVATO

Come già rilevato dal Garante in precedenti occasioni (cfr. pareri del 12 marzo 2003 [doc. web n. 1054779], del 12 maggio 2005 [doc. web n. 1131800] e del 25 luglio 2007 [doc. web n. 1431012]), la particolare ampiezza del novero dei soggetti tenuti ad obblighi di identificazione della clientela, di registrazione delle operazioni e di segnalazione di operazioni sospette impone da tempo una riflessione di fondo sul crescente impatto che la normativa antiriciclaggio assume sempre più in un numero crescente di settori, nonché sulle connesse implicazioni che ne derivano per i diritti delle persone e sul piano della protezione dei dati personali.

A tale riguardo si ritiene opportuno precisare che la direttiva 2015/849 - pur sottolineando che la lotta contro il riciclaggio e il finanziamento del terrorismo è riconosciuta di interesse pubblico rilevante da parte di tutti gli Stati membri (cfr. art. 43) - espressamente cita la necessità di assicurare la protezione dei dati, in ossequio alla direttiva 95/46 (cfr. art. 41, considerando 41 e 42), e stabilisce che la raccolta e il successivo trattamento di dati personali da parte dei soggetti obbligati devono essere limitati a quanto necessario per conformarsi alle prescrizioni della direttiva antiriciclaggio, senza un ulteriore trattamento dei dati personali che sia incompatibile con gli scopi suddetti (art. 41; considerando 43). Inoltre, prevede il categorico divieto di ulteriore trattamento dei dati personali a fini commerciali (considerando 43).

Come già faceva la precedente direttiva 2005/60/CE (c.d. "terza direttiva"), anche la direttiva 2015/849 (c.d. "quarta direttiva"), oggetto di odierna attuazione, pone l'accento sulla necessità di rispettare i diritti fondamentali delle persone e i princìpi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea, il cui articolo 8 garantisce ad ogni individuo il diritto alla protezione dei dati personali che lo riguardano (considerando 43).

In tale quadro, pertanto, si ribadisce al legislatore la necessità (cfr. parere del 25 luglio 2007 [doc. web n. 1431012]) di procedere ad un'attuazione rigorosa in chiave di effettiva necessità, di proporzionalità e di selettività degli interventi di monitoraggio e prevenzione previsti (artt. 2 e 11 del Codice in materia di protezione dei dati personali), anche in considerazione degli enormi flussi informativi previsti, specie verso l'organismo nazionale istituito presso la Banca d'Italia a seguito della direttiva 2005/60 (Unità di Informazione Finanziaria per l'Italia-UIF), e della particolare natura del trattamento.

Lo schema di decreto si compone di 10 articoli: i primi cinque apportano modifiche al d.lgs. 21 novembre 2007, n. 231; gli articoli 6, 7 e 8 introducono modifiche, rispettivamente, al d.lgs. 22 giugno 2007, n. 109, al d.lgs. 19 novembre 2008, n. 195 e ad ulteriori disposizioni vigenti, trasversalmente richiamate dalla normativa di settore.

OSSERVA

Si rappresenta che i seguenti riferimenti all'articolato devono intendersi alla nuova versione del d.lgs. 21 novembre 2007, n. 231, così come modificata dallo schema in esame.

1. Banche dati accessibili da parte dell'Unità di Informazione Finanziaria

L'art. 6, comma 6, riproponendo i contenuti del precedente decreto legislativo, ribadisce che, per l'esercizio delle funzioni di cui ai commi precedenti, la UIF si avvale dei "dati contenuti nell'anagrafe dei conti e dei depositi di cui all'art. 20, comma 4, della legge 30 dicembre 1991, n. 413 e nell'anagrafe tributaria di cui all'articolo 37 del decreto-legge 4 luglio 2006, n. 223". Peraltro, il seguente art. 9, comma 6, lett. a) dello schema definisce, invece, in maniera più precisa la medesima banca dati oggetto di consultazione "dati contenuti nella sezione dell'anagrafe tributaria di cui all'articolo 7, commi 6 e 11 del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, come modificato dall'articolo 37, comma 4, del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248".

Al riguardo, visto il carattere di revisione organica della disciplina antiriciclaggio da parte dello schema in esame, si evidenzia l'esigenza di riformulare tale periodo, anche in considerazione delle intercorse modifiche normative che hanno ampliato i dati sui rapporti finanziari conoscibili dall'UIF, che comprendono ora anche i dati c.d. "contabili" (ad esempio, saldi e giacenza media).

Fermo restando che l'"anagrafe dei conti e dei depositi", seppur disciplinata anche dal d.m. 269/2000, su cui il Garante ha espresso il proprio parere in data 18 novembre 1999, non risulta essere stata implementata, la UIF risulta abilitata a consultare non solo i dati relativi all'esistenza dei rapporti finanziari contenuti nell'apposita sezione "Archivio dei rapporti finanziari" dell'anagrafe tributaria di cui alle predette disposizioni, ma anche i predetti dati contabili (cfr. combinato disposto dagli artt. 7 del d.P.R. 29 settembre 1973 e 11, commi 2, 3 e 4 del d.l. 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214 e, da ultimo, Provvedimento del Direttore dell'Agenzia delle entrate n. 18269/2015 del 2015). L'archivio dei rapporti finanziari, rispetto alla sua prima costituzione, risulta, infatti, oggi ampliato sia in termini di tipologia di rapporti oggetto di comunicazione da parte degli operatori finanziari, che di quantità di informazioni relative al rapporto.

Pertanto, la corretta formulazione dell'art. 6, comma 6, deve riportare gli esatti riferimenti normativi, evidenziando che possono essere consultati anche i dati contabili in aggiunta "ai dati contenuti nella sezione dell'anagrafe tributaria di cui all'articolo 7, commi 6 e 11 del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, come modificato dall'articolo 37, comma 4, del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248, comprese le informazioni di cui all'art. 11, comma 2, del decreto-legge 6 dicembre 2011, n. 201 convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214".

1.1. Modalità di trattamento dei dati da parte della UIF

Nelle disposizioni che regolano i flussi dati tra gli operatori finanziari e la UIF, e quindi determinano la costituzione presso tale soggetto della banca dati delle segnalazioni di operazioni sospette, non è stata rinvenuta un'espressa previsione che imponga alla UIF l'adozione di garanzie e misure in termini di protezione dei dati personali (ci si limita all'individuazione di misure per la riservatezza del segnalante).

Sarebbe opportuno, pertanto, introdurre una disposizione che preveda tra gli obblighi della UIF anche quelli di individuare misure idonee a garantire la protezione dei dati personali nelle comunicazioni dei dati da parte degli operatori finanziari alla UIF e sulla tenuta e gli accessi alla banca dati, da adottare sentito il Garante.

In tale atto regolamentare dovrebbero, inoltre, essere specificate le modalità con cui la UIF comunica al segnalante, direttamente ovvero tramite gli organismi di autoregolamentazione, gli esiti delle segnalazioni (cfr. art. 2 che modifica l'art. 41, comma 2, del d.lgs. 21 novembre 2007, n. 231), oltre agli opportuni criteri di aggregazione e cautele per l'accesso diretto da parte della UIF ai dati e alle informazioni conservate dall'intermediario bancario o finanziario o dalla società fiduciaria (cfr. art. 2 che modifica l'art. 33 del d.lgs. 21 novembre 2007, n. 231).

2. Obblighi di adeguata verifica della clientela

Come già evidenziato nel parere del Garante del 25 luglio 2007 [doc. web n. 1431012], occorre ricordare che la descrizione degli obblighi di adeguata verifica della clientela (art. 18) deve avvenire in termini precisi e conformi alla direttiva europea, al fine di poter trattare solo dati pertinenti e non eccedenti rispetto alle finalità perseguite e con modalità proporzionate (art. 11 del Codice), sia per quanto riguarda

l'identificazione del cliente o del "titolare effettivo", sia in relazione alla valutazione del "rischio" di riciclaggio e di finanziamento del terrorismo.

2.1. Il "sospetto di riciclaggio"

Si ribadisce altresì che lo schema continua a stabilire che i soggetti destinatari delle disposizioni del decreto debbano applicare gli obblighi di adeguata verifica della clientela, fra l'altro, quando vi sia "il sospetto di riciclaggio o di finanziamento del terrorismo" (art. 17, comma 2, lett. a)).

La disposizione lascia un elevato margine di discrezionalità e risulta quindi necessario individuare già nel decreto alcuni criteri, quantomeno generali, da applicare per valutare la sussistenza di tale "sospetto", analogamente o anche mediante rinvio a quanto previsto per la valutazione del "rischio" di riciclaggio e per l'individuazione delle operazioni sospette.

2.2. L'identificazione del cliente

Gli obblighi di adeguata verifica della clientela consistono in alcune attività fra le quali è compresa l'identificazione del cliente e la verifica della sua identità, sulla base di documenti, dati o informazioni ottenuti da una "fonte affidabile e indipendente" (art. 18, comma 1, lett. a), dello schema). Si ritiene necessario sviluppare ulteriormente tale espressione, eventualmente anche mediante una casistica di "fonti", chiarendo altresì se fra di esse siano inclusi, e a quale titolo, terzi che possono contribuire alla verifica della clientela; si deve altresì esplicitare che il trattamento dei dati da parte della "fonte" deve essere comunque lecito, in base alla legge.

3. Modalità di adempimento degli obblighi di adeguata verifica

L'art. 19, comma 1, lett. a), punto 2, sancisce che l'obbligo di identificazione da parte dei soggetti obbligati si considera assolto, anche senza la presenza fisica del cliente, per i clienti in possesso di un'identità digitale di livello massimo di sicurezza nell'ambito del Sistema di cui all'art. 64 del d.lgs. 7 marzo 2005, n. 82.

Si ritiene pertanto opportuno evidenziare che per "livello massimo di sicurezza nell'ambito del Sistema" non si debba intendere quello presente allo stato dei fatti, bensì il livello massimo di sicurezza previsto nell'ambito del sistema Spid, ovvero, attualmente, il livello 3.

3.1. Consultazione dell'archivio SCIPAFI

L'art. 19, comma 1, lett. b), prima parte, contempla l'ipotesi in cui emergano perplessità circa la veridicità dei dati identificativi forniti dal cliente per adempiere agli obblighi di adeguata verifica. In tal caso si prevede che il riscontro della veridicità degli stessi venga effettuato tramite la consultazione del sistema pubblico per la prevenzione del furto di identità di cui d.lgs. 11 aprile 2011, n. 64.

All'art. 8, comma 11, dello schema in esame è poi previsto che all'articolo 30-ter del d.lgs. 13 agosto 2010, n. 141, dopo il comma 5, sia inserito il seguente:"5-bis. Al sistema di prevenzione accedono altresì i soggetti destinatari degli obblighi di adeguata verifica della clientela di cui all'articolo 3 del decreto legislativo 21 novembre 2007, n. 231, e successive modificazioni, non ricompresi tra i soggetti aderenti di cui al comma 5, secondo i termini e le modalità disciplinati in un'apposita convenzione con il Ministero dell'economia e delle finanze, dalla quale non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.".

Al riguardo, si rende opportuno introdurre nella disposizione il rinvio a un decreto modificativo della disciplina attuale di accesso al Sistema SCIPAFI prevista in particolare dal d.m. 19 maggio 2014, n. 95, su cui il Garante ha espresso il proprio parere, per specificare i presupposti, le categorie di soggetti che vi possono accedere, le procedure di abilitazione dei soggetti obbligati e i dati oggetto di riscontro per la verifica della veridicità dei dati forniti. La nuova disposizione potrebbe recitare come segue: "Con decreto del Ministro dell'economia e delle finanze, da adottarsi previo parere del Garante per la protezione dei dati personali, sono individuati i presupposti, le categorie di soggetti che vi possono accedere, nonché il processo di rilascio delle credenziali, i profili di accesso ai dati, le procedure di autenticazione, di registrazione e di analisi degli accessi e delle operazioni per il predetto sistema per la verifica della veridicità dei dati forniti".

3.2. Altre procedure di verifica dell'identità

L'art. 19, comma 1, lett. b), seconda parte, prevede che "la verifica dell'identità può essere effettuata anche attraverso il ricorso ad altre fonti attendibili ed indipendenti tra le quali rientrano le basi di dati ad accesso pubblico o condizionato al rilascio di credenziali di autenticazione, riferibili a una pubblica amministrazione". In proposito occorre rilevare che la disposizione è troppo generica perché non permette di individuare le banche dati pubbliche che dovrebbero essere consultate. Pertanto si ritiene opportuno che sia inserito un rinvio ad un successivo atto regolamentare che le individui, o in mancanza espungere tale periodo dal testo. Ciò in quanto l'accesso a SCIPAFI già consente la verifica dei dati attraverso la consultazione delle banche dati pubbliche, anche ad accesso riservato, idonee a verificare l'identità.

4. Registrazione e conservazione dei dati: la durata della conservazione

Per assicurare il rispetto del principio di conservazione dei dati per il tempo strettamente necessario al raggiungimento delle finalità, come già affermato nel parere del 2007, si ritiene necessaria un'attenta rivalutazione sulla effettiva congruità del periodo "di almeno dieci anni" individuato nello schema per la conservazione della documentazione (art. 31 e ss. dello schema).

Come già affermato dal Garante al riguardo, si rileva anzitutto la non praticabilità di un termine di conservazione sostanzialmente indefinito, quale quello che deriva, allo stato, dall'impiego dell'espressione "almeno" che, per esigenze di certezza, va eliminata prevedendo un chiaro termine finale di conservazione.

Con riferimento a tale termine, si sottolinea, inoltre, che la direttiva europea si limita a stabilire un termine di "almeno cinque anni" dalla fine del rapporto d'affari o dall'esecuzione dell'operazione (art. 40 direttiva (UE) 2015/849); allo stato, non risulta altresì alcuna concreta dimostrazione dell'effettiva necessità di prevedere un termine in ogni caso non inferiore al doppio del termine mimino armonizzato su scala europea.

Si ritiene, poi, necessaria una rivalutazione sulla congruità del periodo "di dieci anni" per il quale è previsto che la UIF conservi in "evidenza" le segnalazioni ritenute infondate, tenuto conto anche del fatto che si tratterebbe di informazioni già valutate come non rilevanti ai fini del contrasto del riciclaggio (art. 40, comma 1, lett. d), dello schema).

5. Misure di sicurezza per comunicazione e conservazione

In linea generale si ritiene opportuno effettuare nello schema di decreto un espresso richiamo al d.P.C.M. del 22 febbraio 2013 che stabilisce le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi del CAD, per ciò che riguarda l'utilizzo della firma digitale, oltre che al d.P.C.M. del 13 novembre 2014 sulle "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005", per ciò che riguarda le modalità di conservazione dei dati e delle informazioni (cfr. art. 32 del d.lgs. 21 novembre 2007, n. 231).

5.1. Conservazione da parte dei soggetti obbligati

L'art. 32, comma 1, prescrive agli operatori finanziari di "adottare sistemi di conservazione dei documenti, dati e informazioni idonei a garantire il rispetto delle norme dettate dal codice in materia di dati personali". A tal proposito, analogamente a quanto già prescritto dal Garante in sede di parere sulla comunicazione dei dati all'archivio dei rapporti finanziari (parere del 15 novembre 2012 [doc. web n. 2099774], si ritiene opportuno richiamare anche nel decreto oggetto del presente parere le seguenti misure di sicurezza affinché:

a) i soggetti che trattano i dati siano scelti dagli operatori finanziari sulla base di elevati requisiti di idoneità soggettiva in termini di affidabilità e competenze, preferibilmente tra coloro che abbiano un rapporto stabile con essi;

b) anche in considerazione delle dimensioni dell'operatore finanziario, siano adottati meccanismi di cifratura e di sicurezza, rispettivamente finalizzati a proteggere le informazioni contenute nei file e ad assicurare l'integrità del contenuto e a prevenirne alterazioni;

c) l'accesso alle informazioni in tutte le fasi del trattamento, anche dopo la cifratura, sia circoscritto ad un numero il più possibile limitato di incaricati;

d) qualora gli operatori finanziari decidano di affidare la comunicazione a soggetti esterni, designati responsabili o incaricati del trattamento, i dati siano loro forniti già cifrati.

5.2. Conservazione da parte di soggetti esterni

L'art. 32, comma 3, consente ai soggetti obbligati di avvalersi di un autonomo centro di servizi, ovvero di un soggetto esterno, per la conservazione di documenti, dati e informazioni, purché sia assicurato ai soggetti obbligati l'accesso diretto e immediato al sistema di conservazione. Con riferimento al ruolo assunto dal centro di servizi, rispetto al trattamento dei dati personali, occorre prescrivere che:

a) tale soggetto sia preventivamente designato quale responsabile del trattamento, che deve offrire idonee garanzie in relazione a quanto previsto dall'art. 29 del Codice;

b) siano fornite a tale soggetto adeguate istruzioni;

c) il titolare vigili sul trattamento da effettuare, con particolare riguardo alle ipotesi in cui tale soggetto sia designato responsabile da più operatori, al fine di garantire misure di carattere tecnico organizzativo volte ad assicurare la segregazione dei flussi con ciascun operatore.

5.3. Ulteriori misure tecnico/organizzative

Sempre con riferimento ai profili tecnico/organizzativi, connessi al trattamento di dati personali, si ritiene opportuno integrare le disposizioni dello schema di decreto, prevedendo in particolare che vengano:

a) previste adeguate modalità di gestione della c.d. "lista nazionale" che riguarda la designazione di persone o entità e il conseguente congelamento dei loro fondi e risorse economiche (cfr. art. 6 che introduce il nuovo art. 4-bis nel d.lgs. 22 giugno 2007, n. 109);

b) adottati accorgimenti e misure a protezione dei dati personali per la notifica, mediante posta elettronica certificata, da parte del Nucleo speciale polizia valutaria della Guardia di finanza ai soggetti designati dell'avvenuto congelamento delle risorse economiche e della loro successiva assunzione da parte dell'Agenzia del demanio (cfr. art. 6 che modifica l'art. 11 del d.lgs. 22 giugno 2007, n. 109).

Infine, per assicurare una disciplina omogenea della materia è opportuno che, qualora i diversi decreti attuativi, regole o specifiche tecniche,

protocolli di intesa e convenzioni citati nello schema di decreto prevedano anche una disciplina sulla riservatezza delle informazioni, i medesimi atti vengano adottati su conforme parere del Garante.

TUTTO CIÒ PREMESSO IL GARANTE

esprime parere favorevole sullo schema di decreto legislativo recante disposizioni per il recepimento della direttiva (UE) 2015/849 (c.d. "quarta direttiva"), concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, evidenziando in particolare quanto rappresentato al punto 2.1. e a condizione che lo schema sia modificato, nei termini di cui in motivazione:

a) introdurre una disposizione che preveda tra gli obblighi dell'UIF anche quelli di individuare misure idonee a garantire la protezione dei dati personali nelle comunicazioni dei dati da parte degli operatori finanziari all'UIF e sulla tenuta e gli accessi alla banca dati, da adottare sentito il Garante (punto 1.1.);

b) prevedere una nuova disposizione che rimandi ad un decreto modificativo della disciplina attuale di accesso al Sistema SCIPAFI prevista in particolare dal d.m. 19 maggio 2014, n. 95 che, previo parere del Garante, individui i presupposti, le categorie di soggetti che vi possono accedere, le procedure di abilitazione dei soggetti obbligati e i dati oggetto di riscontro per la verifica della veridicità dei dati forniti (punto 3.1.);

c) inserire all'art. 19, comma 1, lett. b), seconda parte un rinvio ad un successivo atto regolamentare che individui le banche dati pubbliche che dovrebbero essere consultate, ovvero espungere tale periodo dal testo, tenendo conto del fatto che già l'accesso a SCIPAFI consente la verifica dei dati attraverso la consultazione delle banche dati pubbliche, anche ad accesso riservato, idonee a verificare l'identità (3.2.);

d) ridurre, inserendo un termine certo, la durata della conservazione dei dati (punto 4.);

e) inserire il richiamo al d.P.C.M. del 22 febbraio 2013 e al d.P.C.M. del 13 novembre 2014 (punto 5.);

f) richiamare le misure di sicurezza di cui al punto 5.1. e 5.2.;

g) prevedere adeguate modalità di gestione della c.d. "lista nazionale" che riguarda la designazione di persone o entità e il conseguente congelamento dei loro fondi e risorse economiche (punto 5.3.);

h) adottare accorgimenti e misure a protezione dei dati personali per la notifica, mediante posta elettronica certificata, da parte del Nucleo speciale polizia valutaria della Guardia di finanza ai soggetti designati dell'avvenuto congelamento delle risorse economiche e della loro successiva assunzione da parte dell'Agenzia del demanio (punto 5.3.).

Roma, 9 marzo 2017

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia