REGOLAMENTO DELEGATO (UE) 2017/571 DELLA COMMISSIONE

del 2 giugno 2016

che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione sull'autorizzazione, i requisiti organizzativi e la pubblicazione delle operazioni per i fornitori di servizi di comunicazione dati

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE ([1]), in particolare l'articolo 61, paragrafo 4, l'articolo 64, paragrafi 6 e 8, l'articolo 65, paragrafi 6 e 8, e l'articolo 66, paragrafo 5,

considerando quanto segue:

(1) A norma della direttiva 2014/65/UE si considerano fornitori di servizi di comunicazione dati tre tipi di soggetti diversi: i meccanismi di segnalazione autorizzati (ARM), i dispositivi di pubblicazione autorizzati (APA) e i fornitori di sistemi consolidati di pubblicazione (CTP). Sebbene questi tipi di soggetti svolgano attività diverse, la direttiva 2014/65/UE prevede per tutti una procedura di autorizzazione simile.

(2) Il richiedente l'autorizzazione come fornitore di servizi di comunicazione dati dovrebbe indicare nella domanda il programma di attività e l'organigramma. L'organigramma dovrebbe indicare i responsabili delle diverse attività per consentire all'autorità competente di valutare se il fornitore di servizi di comunicazione dati disponga di risorse umane sufficienti e eserciti una sorveglianza adeguata sull'attività svolta. L'organigramma dovrebbe riportare non solo la gamma coperta dai servizi di comunicazione dati, ma anche tutti gli altri servizi prestati, in quanto una tale presentazione permetterebbe di evidenziare i settori che, potendo incidere sull'indipendenza del fornitore di servizi di comunicazione dati, potrebbero essere all'origine di conflitti di interesse. Il richiedente l'autorizzazione come fornitore di servizi di comunicazione dati dovrebbe fornire anche informazioni sulla composizione, il funzionamento e l'indipendenza dei suoi organi di gestione, in modo da consentire alle autorità competenti di valutare se le politiche, le procedure e la struttura di governo societario garantiscano l'indipendenza del fornitore di servizi di comunicazione dati e impediscano l'insorgere di conflitti di interesse.

(3) Possono insorgere conflitti di interesse tra il fornitore di servizi di comunicazione dati e i clienti che si avvalgono dei suoi servizi per rispettare obblighi di legge e altri soggetti che acquistano dati da fornitori di servizi di comunicazione dati. In particolare, possono sorgere conflitti di interesse quando il fornitore di servizi di comunicazione dati svolge altre attività in qualità di gestore del mercato, impresa di investimento o repertorio di dati sulle negoziazioni. Se i conflitti di interesse non sono risolti possono crearsi situazioni in cui il fornitore di servizi di comunicazione dati è incentivato a ritardare la pubblicazione o la trasmissione dei dati o a realizzare operazioni sulla base delle informazioni riservate ricevute. Il fornitore di servizi di comunicazione dati dovrebbe pertanto adottare un approccio globale per individuare, prevenire e gestire i conflitti di interesse esistenti e potenziali, anche compilando un inventario dei conflitti di interesse e attuando politiche e procedure appropriate per gestirli e, se necessario, separare aree di attività e membri del personale così da limitare il flusso di informazioni sensibili tra i propri diversi settori di attività.

(4) Tutti i membri dell'organo di gestione del fornitore di servizi di comunicazione dati dovrebbero essere persone che soddisfano i requisiti di onorabilità e possiedono le conoscenze, le competenze e l'esperienza necessarie, perché hanno un ruolo essenziale nel garantire che il fornitore di servizi di comunicazione dati rispetti gli obblighi che gli sono imposti dalla legge e nel contribuire alla strategia aziendale del fornitore di servizi di comunicazione dati. Pertanto, è importante che il fornitore di servizi di comunicazione dati dimostri di essersi dotato di una solida procedura di nomina e di valutazione delle prestazioni dei membri dell'organo di gestione e di aver predisposto chiare linee gerarchiche e chiare disposizioni in materia di informazione regolare all'organo di gestione.

([1]) GU L 173 del 12.6.2014, pag. 349.

(5) L'esternalizzazione delle attività, in particolare delle funzioni essenziali, può costituire una modifica rilevante delle condizioni cui è subordinata l'autorizzazione del fornitore di servizi di comunicazione dati. Per assicurare che l'esternalizzazione delle attività non comprometta la sua capacità di adempiere gli obblighi di cui alla direttiva 2014/65/UE né faccia sorgere conflitti di interesse, il fornitore di servizi di comunicazione dati dovrebbe poter dimostrare di esercitare su dette attività una sorveglianza e un controllo adeguati.

(6) I sistemi informatici usati dal fornitore di servizi di comunicazione dati dovrebbero essere adatti ai diversi tipi di attività che il fornitore può svolgere, ossia pubblicare report delle operazioni concluse, presentare rendiconti delle operazioni o fornire un sistema consolidato di pubblicazione, e sufficientemente solidi da assicurare la continuità e la regolarità della prestazione di detti servizi. Ciò significa tra l'altro assicurare che il sistema informatico del fornitore di servizi di comunicazione dati sia in grado di assorbire le fluttuazioni del volume di dati da gestire. Tali fluttuazioni, in particolare un aumento inaspettato del flusso di dati, possono avere un impatto negativo sull'efficienza dei sistemi del fornitore di servizi di comunicazione dati e, di conseguenza, sulla sua capacità di pubblicare o comunicare informazioni complete e corrette nei termini previsti. Per ovviare a questa situazione il fornitore di servizi di comunicazione dati dovrebbe sottoporre a prova periodica i suoi sistemi, per assicurarsi che siano sufficientemente solidi da assorbire le variazioni delle condizioni operative e sufficientemente scalabili.

(7) I dispositivi e le modalità di back-up predisposti dal fornitore di servizi di comunicazione dati dovrebbero essere atti a consentirgli di prestare i servizi anche in caso di evento perturbatore. Il fornitore di servizi di comunicazione dati dovrebbe fissare i tempi massimi accettabili di ripristino delle funzioni essenziali applicabili in caso di evento perturbatore, che dovrebbero consentire di rispettare i termini di segnalazione e di informativa.

(8) Per assicurarsi di poter prestare i servizi, il fornitore di servizi di comunicazione dati dovrebbe effettuare un'analisi dei compiti e delle attività essenziali per fornirli e delle situazioni che potrebbero dare luogo a un evento perturbatore, anche adottando misure per prevenirlo e attenuarlo.

(9) Nel caso in cui si verifichi un'interruzione del servizio, il fornitore di servizi di comunicazione dati dovrebbe darne notifica all'autorità competente del proprio Stato membro d'origine, a tutte le altre autorità competenti interessate, ai clienti e al pubblico, dato che l'interruzione potrebbe anche impedire a dette parti di adempiere gli obblighi di legge che incombono loro, quali l'obbligo di inoltrare i rendiconti delle operazioni ad altre autorità competenti o di rendere pubblici i particolari delle operazioni effettuate. La notifica dovrebbe consentire a dette parti di mettere in atto dispositivi alternativi per rispettare gli obblighi che incombono loro.

(10) Gli aggiornamenti dei sistemi informatici possono influire sull'efficacia e la solidità dei sistemi utilizzati per la fornitura dei servizi di dati. Per evitare che il funzionamento del suo sistema informatico risulti in un qualsiasi momento incompatibile con gli obblighi di legge, in particolare l'obbligo di disporre di un efficace meccanismo di sicurezza finalizzato a garantire la sicurezza dei mezzi per il trasferimento delle informazioni, a minimizzare i rischi di corruzione dei dati e a prevenire la fuga di informazioni prima della pubblicazione, il fornitore di servizi di comunicazione dati dovrebbe impiegare metodologie di sviluppo e di prova ben delineate per assicurare che i controlli della conformità e della gestione dei rischi incorporati nel sistema funzionino come previsto e che il sistema possa continuare a funzionare in maniera efficiente in tutte le situazioni. Se introduce una modifica significativa nel sistema, il fornitore di servizi di comunicazione dati dovrebbe darne notifica all'autorità competente del proprio Stato membro d'origine e alle eventuali altre autorità competenti, in modo che possano valutare se l'aggiornamento inciderà sui loro sistemi e se le condizioni dell'autorizzazione restino soddisfatte.

(11) Un'informativa al pubblico prematura, nel caso dei report delle operazioni concluse, o un'informativa non autorizzata, nel caso dei rendiconti delle operazioni, potrebbero fornire un'indicazione della strategia di negoziazione o rivelare informazioni sensibili quali l'identità dei clienti del fornitore di servizi di comunicazione dati. Pertanto, il fornitore di servizi di comunicazione dati dovrebbe predisporre controlli fisici, quali spazi chiusi a chiave, e controlli elettronici, compresi firewall e password, in modo che solo il personale autorizzato abbia accesso ai dati.

(12) Le violazioni della sicurezza fisica o elettronica del fornitore di servizi di comunicazione dati costituiscono una minaccia per la riservatezza dei dati dei clienti. Quando si verifica una tale violazione, il fornitore di servizi di comunicazione dati dovrebbe pertanto darne immediata notifica all'autorità competente interessata e ai clienti

che ne subiscono le conseguenze. La notifica all'autorità competente dello Stato membro d'origine è necessaria per consentirle di svolgere i suoi compiti di vigilanza continua verificando se il fornitore di servizi di comunicazione dati mantenga adeguatamente efficaci meccanismi di sicurezza atti a garantire la sicurezza delle informazioni e minimizzare i rischi di corruzione dei dati e di accesso non autorizzato. Dovrebbe essere data notifica anche alle altre autorità competenti che hanno un'interfaccia tecnica con il fornitore di servizi di comunicazione dati, dato che potrebbero risentire negativamente della violazione, soprattutto quando questa riguarda i mezzi per il trasferimento delle informazioni tra il fornitore di servizi di comunicazione dati e l'autorità competente.

(13) L'impresa di investimento che ha l'obbligo di segnalare le operazioni («impresa segnalante») può scegliere di incaricare un terzo («impresa trasmittente») di trasmettere per suo conto i rendiconti delle operazioni a un ARM. Dato il ruolo che riveste, l'impresa trasmittente avrà accesso alle informazioni riservate che trasmette. L'impresa trasmittente non dovrebbe tuttavia poter accedere agli altri dati sull'impresa segnalante o sulle operazioni dell'impresa segnalante detenute dall'ARM. Tali dati possono riguardare i rendiconti delle operazioni che l'impresa segnalante ha trasmesso all'ARM in prima persona o per il tramite di un'altra impresa trasmittente. Tali dati non dovrebbero essere accessibili all'impresa trasmittente perché possono contenere informazioni riservate, quali l'identità dei clienti dell'impresa segnalante.

(14) Il fornitore di servizi di comunicazione dati dovrebbe controllare che i dati che pubblica o trasmette siano corretti e completi e dovrebbe assicurarsi di disporre di meccanismi per individuare gli errori od omissioni attribuibili al cliente o ad esso stesso. Nel caso degli ARM può trattarsi di riconciliazioni tra una popolazione campione di dati trasmessi all'ARM da un'impresa di investimento, o generati dall'ARM per conto dell'impresa di investimento, e i corrispondenti dati forniti dall'autorità competente. La frequenza e la portata delle riconciliazioni dovrebbero essere proporzionate al volume dei dati trattati dall'ARM e alla misura in cui questo genera rendiconti delle operazioni a partire dai dati dei clienti o trasmette rendiconti delle operazioni compilati dai clienti. Per assicurare segnalazioni tempestive prive di errori o omissioni, l'ARM dovrebbe monitorare costantemente le prestazioni dei suoi sistemi.

(15) Se è esso stesso all'origine di un errore o omissione, l'ARM dovrebbe correggere prontamente il dato e notificare l'errore o omissione all'autorità competente del proprio Stato membro d'origine e alle altre autorità competenti alle quali trasmette segnalazioni, perché la qualità dei dati che ricevono riveste interesse per tali autorità. L'ARM dovrebbe notificare l'errore o omissione anche al cliente comunicandogli le informazioni aggiornate in modo che possa allineare la documentazione interna alle informazioni che l'ARM ha trasmesso per suo conto all'autorità competente.

(16) È opportuno che gli APA e i CTP possano cancellare e modificare le informazioni ricevute da un soggetto per risolvere, in casi eccezionali, le situazioni in cui difficoltà tecniche impediscono al soggetto segnalante di cancellare o modificare direttamente tali informazioni. Negli altri casi gli APA e i CTP non dovrebbero tuttavia essere responsabili della correzione delle informazioni contenute nei report o rendiconti pubblicati quando l'errore o l'omissione è attribuibile al soggetto che le fornisce perché, non essendo parti della negoziazione eseguita, l'APA e il CTP non possono avere la certezza che quello che percepiscono come errore o omissione sia effettivamente errato.

(17) Ai fini di una comunicazione affidabile tra l'APA e l'impresa di investimento che segnala una negoziazione conclusa, in particolare per quanto riguarda l'annullamento e la modifica di specifiche operazioni, l'APA dovrebbe inserire nel messaggio di conferma inviato all'impresa di investimento segnalante il codice identificativo che ha assegnato all'operazione al momento della pubblicazione dell'informazione.

(18) Per rispettare l'obbligo di segnalazione impostogli dal regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio ([1]), l'ARM dovrebbe assicurare il flusso regolare delle informazioni verso le autorità competenti e da queste proveniente, compresa la capacità di trasferire le segnalazioni e di trattare le segnalazioni respinte. L'ARM dovrebbe pertanto essere in grado di dimostrare di poter rispettare le specifiche tecniche stabilite dall'autorità competente per quanto riguarda l'interfaccia tra di esso e l'autorità competente.

([1]) Regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 (GU L 173 del 12.6.2014, pag. 84).

(19) Il fornitore di servizi di comunicazione dati dovrebbe provvedere a conservare le informazioni relative ai rendiconti delle operazioni e ai report delle operazioni concluse trattati, per un periodo di tempo sufficientemente lungo da permettere alle autorità competenti di reperire più agevolmente i dati storici. Gli APA e i CTP dovrebbero provvedere a predisporre le necessarie disposizioni organizzative per conservare i dati almeno per il periodo previsto dal regolamento (UE) n. 600/2014 e a essere in grado di soddisfare qualsiasi richiesta di prestazione dei servizi disciplinati dal presente regolamento.

(20) Il presente regolamento prevede una serie di servizi aggiuntivi di miglioramento dell'efficienza del mercato che potrebbero essere prestati dai CTP. In considerazione della possibile evoluzione del mercato, non è opportuno compilare un elenco esaustivo dei servizi aggiuntivi che potrebbero prestare i CTP. Il CTP dovrebbe pertanto essere in grado di fornire altri servizi oltre agli specifici servizi aggiuntivi elencati nel presente regolamento, a condizione tuttavia che questi altri servizi non mettano a rischio l'indipendenza del CTP né la qualità del sistema consolidato di pubblicazione.

(21) Affinché le informazioni possano essere diffuse efficacemente e i partecipanti al mercato possano accedervi agevolmente e usarle, gli APA e i CTP dovrebbero pubblicarle in linguaggio macchina attraverso canali solidi che consentano l'accesso automatico ai dati. Sebbene i siti web non sempre offrano un'architettura sufficientemente solida e scalabile che consente un agevole accesso automatico ai dati, questi vincoli tecnologici potranno essere superati in futuro. Piuttosto che imporre una particolare tecnologia, è opportuno stabilire i criteri che la tecnologia usata deve soddisfare.

(22) Per gli strumenti rappresentativi di capitale e gli strumenti simili a quelli rappresentativi di capitale il regolamento (UE) n. 600/2014 non esclude la possibilità che le imprese di investimento ricorrano a più di un APA per rendere pubbliche le operazioni eseguite. Dovrebbero essere tuttavia predisposte modalità specifiche che permettano alle parti interessate che consolidano le informazioni sulle negoziazioni provenienti dai diversi APA, in particolare ai CTP, di individuare i potenziali duplicati, per evitare che la stessa negoziazione sia consolidata più volte e che i CTP ne replichino la pubblicazione, con conseguenze negative per la qualità e l'utilità del sistema consolidato di pubblicazione.

(23) L'APA dovrebbe pertanto pubblicare le operazioni segnalate dalle imprese di investimento inserendovi, all'atto della pubblicazione, un campo «ristampa» in cui indica che si tratta di un duplicato della segnalazione. Ai fini della neutralità tecnologica è necessario prevedere diversi modi in cui l'APA possa individuare i duplicati.

(24) Per assicurare che ogni operazione sia inserita solo una volta nel sistema consolidato di pubblicazione e per migliorare quindi l'attendibilità delle informazioni fornite, i CTP non dovrebbero pubblicare informazioni sulle operazioni pubblicate da un APA e contrassegnate come duplicati.

(25) L'APA dovrebbe pubblicare informazioni sull'operazione comprensive delle opportune marche temporali, quali ad esempio il momento in cui è stata eseguita e quello in cui è stata segnalata. Inoltre, il livello di dettaglio delle marche temporali dovrebbe rispecchiare la natura del sistema di negoziazione in cui l'operazione è stata eseguita. Nel caso di pubblicazione di informazioni sulle operazioni eseguite in sistemi elettronici dovrebbe essere offerto un livello di dettaglio maggiore che per le operazioni eseguite in sistemi non elettronici.

(26) I CTP possono pubblicare informazioni sugli strumenti di capitale e sugli strumenti diversi dagli strumenti di capitale. Dati i diversi requisiti di funzionamento dei sistemi di pubblicazione, in particolare l'ambito notevolmente più ampio degli strumenti diversi dagli strumenti di capitale coperti e l'applicazione differita delle disposizioni della direttiva 2014/65/UE per il sistema consolidato di pubblicazione degli strumenti diversi dagli strumenti di capitale, il presente regolamento si limita a specificare la portata delle informazioni sugli strumenti di capitale che il CTP deve consolidare.

(27) Le disposizioni del presente regolamento sono strettamente correlate, in quanto vertono sull'autorizzazione, i requisiti organizzativi e la pubblicazione delle operazioni per i fornitori di servizi di comunicazione dati. Per garantire la coerenza tra dette disposizioni, che dovrebbero entrare in vigore contemporaneamente, e per offrire una visione globale ai portatori d'interesse, in particolare alle persone soggette agli obblighi in questione, è necessario riunire le norme tecniche di regolamentazione in un unico regolamento.

(28) Il presente regolamento specifica gli obblighi di pubblicazione dei dati a carico degli APA e dei CTP. Per assicurare prassi uniformi di pubblicazione delle informazioni sulle negoziazioni fra le sedi di negoziazione, gli APA e i CTP e per facilitare il consolidamento dei dati da parte dei CTP, il presente regolamento dovrebbe applicarsi in combinato disposto con i regolamenti delegati della Commissione (UE) 2017/587 ([1]) e (UE) 2017/583 ([2]) in cui sono definiti i requisiti dettagliati per la pubblicazione delle informazioni sulle negoziazioni.

(29) A fini di coerenza e per assicurare il corretto funzionamento dei mercati finanziari, è necessario che le disposizioni del presente regolamento e le collegate disposizioni nazionali di recepimento della direttiva 2014/65/UE si applichino a decorrere dalla stessa data. Dato che l'articolo 65, paragrafo 2, della direttiva 2014/65/UE si applica a decorrere dal 3 settembre dell'anno successivo all'anno di applicazione del presente regolamento, alcune disposizioni del presente regolamento dovrebbero applicarsi da detta data successiva.

(30) Il presente regolamento si basa sui progetti di norme tecniche di regolamentazione che l'Autorità europea degli strumenti finanziari e dei mercati (ESMA) ha presentato alla Commissione.

(31) L'ESMA ha condotto una consultazione pubblica aperta sui progetti di norme tecniche di regolamentazione sui quali è basato il presente regolamento, ha analizzato i potenziali costi e benefici collegati e ha chiesto il parere del gruppo delle parti interessate nel settore degli strumenti finanziari e dei mercati istituito dall'articolo 37 del regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio ([3]),

HA ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

AUTORIZZAZIONE

(Articolo 61, paragrafo 2, della direttiva 2014/65/UE)

Articolo 1

Informazioni alle autorità competenti

1. Il richiedente l'autorizzazione come fornitore di servizi di comunicazione dati trasmette all'autorità competente le informazioni previste agli articoli 2, 3 e 4 e le informazioni su tutti i requisiti organizzativi previste ai capi II e III.

2. Il fornitore di servizi di comunicazione dati informa immediatamente l'autorità competente del proprio Stato membro d'origine di qualsiasi modifica rilevante delle informazioni fornite al momento dell'autorizzazione e successivamente.

Articolo 2

Informazioni sull'organizzazione

1. Il richiedente l'autorizzazione come fornitore di servizi di comunicazione dati include nella domanda di autorizzazione il programma di attività previsto all'articolo 61, paragrafo 2, della direttiva 2014/65/UE. Il programma di attività riporta le informazioni seguenti:

a) informazioni sulla struttura organizzativa del richiedente, compresi l'organigramma e la specificazione delle risorse umane, tecniche e giuridiche assegnate alle diverse attività svolte;

([1]) Regolamento delegato (UE) 2017/587 della Commissione, del 14 luglio 2016, che integra il regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio sui mercati degli strumenti finanziari per quanto riguarda le norme tecniche di regolamentazione sugli obblighi di trasparenza a carico delle sedi di negoziazione e delle imprese di investimento relativamente ad azioni, certificati di deposito, fondi indicizzati quotati (ETF), certificati e altri strumenti finanziari analoghi e sull'obbligo di eseguire le operazioni su talune azioni nelle sedi di negoziazione o tramite gli internalizzatori sistematici (cfr. pag. 387 della presente Gazzetta ufficiale).

([2]) Regolamento delegato (UE) 2017/583 della Commissione, del 14 luglio 2016, che integra il regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio sui mercati degli strumenti finanziari per quanto riguarda le norme tecniche di regolamentazione sugli obblighi di trasparenza a carico delle sedi di negoziazione e delle imprese di investimento in relazione a obbligazioni, strumenti finanziari strutturati, quote di emissione e derivati (cfr. pag. 229 della presente Gazzetta ufficiale).

([3]) Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione (GU L 331 del 15.12.2010, pag. 84).

b) informazioni sulle politiche e procedure in materia di conformità attuate dal fornitore di servizi di comunicazione dati, tra cui:

   i) il nome della persona o delle persone responsabili dell'approvazione e del mantenimento di dette politiche;

   ii) le modalità di monitoraggio e effettiva applicazione delle politiche e procedure in materia di conformità;

   iii) i provvedimenti di cui è prospettata l'adozione in caso di violazione che possa determinare l'inadempimento delle condizioni di ottenimento dell'autorizzazione iniziale;

   iv) la descrizione della procedura con cui è segnalata all'autorità competente la violazione che possa determinare l'inadempimento delle condizioni di ottenimento dell'autorizzazione iniziale;

c) un elenco di tutte le funzioni esternalizzate e delle risorse assegnate al controllo delle funzioni esternalizzate.

2. Il fornitore di servizi di comunicazione dati che offre altri servizi oltre a quelli di comunicazione dati descrive detti servizi nell'organigramma.

Articolo 3

Governo societario

1. Il richiedente l'autorizzazione come fornitore di servizi di comunicazione dati include nella domanda informazioni sulle politiche e procedure interne di governo societario che presiedono al suo organo di gestione, all'alta dirigenza e, se costituiti, ai comitati.

2. Le informazioni di cui al paragrafo 1 riportano:

a) la descrizione delle procedure di selezione, nomina, valutazione delle prestazioni e destituzione dell'alta dirigenza e dei membri dell'organo di gestione;

b) la descrizione delle linee gerarchiche e la frequenza con cui sono informati l'alta dirigenza e l'organo di gestione;

c) la descrizione delle politiche e delle procedure in materia di accesso ai documenti da parte dei membri dell'organo di gestione.

Articolo 4

Informazioni sui membri dell'organo di gestione

1. Il richiedente l'autorizzazione come fornitore di servizi di comunicazione dati include nella domanda, per ciascun membro dell'organo di gestione, le informazioni seguenti:

a) nome, data e luogo di nascita, numero di identificazione personale nazionale o codice equivalente, indirizzo e estremi di contatto;

b) funzione che è o sarà ricoperta dalla persona;

c) curriculum vitae comprovante il possesso di esperienza e conoscenze sufficienti ad assolvere adeguatamente i compiti previsti;

d) informazioni sui precedenti penali, in particolare accludendo l'estratto del casellario giudiziale o, se questo non è disponibile nello Stato membro interessato, un'autocertificazione del possesso dei requisiti di onorabilità corredata di una dichiarazione che autorizza l'autorità competente a verificare se la persona abbia subito condanne penali per reati connessi alla prestazione di servizi finanziari o di gestione di dati ovvero per frode o appropriazione indebita;

e) autocertificazione del possesso dei requisiti di onorabilità corredata di una dichiarazione che autorizza l'autorità competente a verificare se la persona:

   i) sia incorsa in una sanzione a conclusione di un procedimento disciplinare avviato nei suoi confronti da un'autorità di regolamentazione o da un organismo pubblico o sia sottoposta a un tale procedimento non ancora concluso;

ii) sia stata condannata in un procedimento giudiziario civile connesso alla prestazione di servizi finanziari o di gestione di dati ovvero per condotta scorretta o frode nella gestione di un'impresa;

iii) abbia fatto parte dell'organo di gestione di un'impresa che è stata condannata o sanzionata da un'autorità di regolamentazione o la cui registrazione o autorizzazione è stata revocata da un'autorità di regolamentazione;

iv) si sia vista rifiutare il diritto di svolgere attività che richiedono la registrazione o l'autorizzazione di un'autorità di regolamentazione;

v) abbia fatto parte dell'organo di gestione di un'impresa dichiarata insolvente o liquidata mentre la persona ricopriva tale funzione o entro un anno dopo che ha cessato di ricoprirla;

vi) sia stata altrimenti multata, sospesa, interdetta o soggetta ad altra sanzione da parte di un organismo professionale per frode o appropriazione indebita ovvero in connessione alla prestazione di servizi finanziari o di gestione di dati;

vii) sia stata esclusa dalla funzione di amministratore o dal ruolo di dirigente, licenziata o rimossa da altro incarico in un'impresa in seguito a condotta scorretta o irregolarità;

f) tempo minimo che la persona è tenuta a dedicare all'esercizio delle funzioni presso il fornitore di servizi di comunicazione dati;

g) dichiarazione dei potenziali conflitti di interesse che esistono o possono sorgere nell'esercizio delle funzioni e indicazione del modo in cui sono gestiti.

CAPO II

REQUISITI ORGANIZZATIVI

(Articolo 64, paragrafi 3, 4 e 5, articolo 65, paragrafi 4, 5 e 6, e articolo 66, paragrafi 2, 3 e 4, della direttiva 2014/65/UE)

Articolo 5

Conflitti di interesse

1. Il fornitore di servizi di comunicazione dati adotta e mantiene disposizioni amministrative efficaci al fine di evitare conflitti di interesse con i clienti che si avvalgono dei suoi servizi per rispettare gli obblighi di legge e altri soggetti che acquistano dati da fornitori di servizi di comunicazione dati. Dette disposizioni includono politiche e procedure per individuare, gestire e dichiarare i conflitti di interesse esistenti e potenziali e prevedono:

a) un inventario dei conflitti di interesse esistenti e potenziali che ne contiene la descrizione, l'individuazione, la prevenzione, la gestione e la dichiarazione;

b) la separazione delle funzioni e delle aree di attività presso il fornitore di servizi di comunicazione dati, tra cui:

i) le misure per impedire o controllare lo scambio di informazioni qualora possa sorgere un rischio di conflitto di interesse;

ii) la vigilanza separata sui soggetti rilevanti le cui principali funzioni implicano interessi in potenziale conflitto con quelli di un cliente;

c) la descrizione della politica tariffaria per determinare le commissioni addebitate dal fornitore di servizi di comunicazione dati e dalle imprese con cui questo ha stretti legami;

d) la descrizione della politica retributiva per i membri dell'organo di gestione e l'alta dirigenza;

e) le regole sull'accettazione di denaro, regalie o favori da parte del personale del fornitore di servizi di comunicazione dati e del relativo organo di gestione.

2. L'inventario dei conflitti di interesse previsto al paragrafo 1, lettera a), elenca i conflitti di interesse derivanti da situazioni in cui il fornitore di servizi di comunicazione dati:

a) può realizzare un guadagno finanziario o evitare una perdita finanziaria a danno di un cliente;

b) può avere nel risultato del servizio prestato a un cliente un interesse distinto da quello del cliente;

c) può avere un incentivo a privilegiare i propri interessi, o gli interessi di un altro cliente o gruppo di clienti, rispetto a quelli del cliente cui presta il servizio;

d) riceve o può ricevere da un terzo, in relazione al servizio fornito a un cliente, un incentivo sotto forma di denaro, di beni o di servizi diverso dalle commissioni o provvigioni addebitate per il servizio.

Articolo 6

Requisiti organizzativi per l'esternalizzazione

1. Se dispone che un terzo, comprese le imprese con cui ha stretti legami, esegua attività per suo conto, il fornitore di servizi di comunicazione dati si accerta che il terzo prestatore di servizi possieda la competenza e la capacità per eseguirle in maniera affidabile e professionale.

2. Il fornitore di servizi di comunicazione dati indica le attività destinate all'esternalizzazione specificando l'entità delle risorse umane e tecniche necessarie per eseguirle.

3. Il fornitore di servizi di comunicazione dati che esternalizza attività provvede a che l'esternalizzazione non limiti la sua capacità o il suo potere di esercitare le funzioni dell'alta dirigenza o dell'organo di gestione.

4. Il fornitore di servizi di comunicazione dati resta responsabile delle attività esternalizzate e adotta i provvedimenti organizzativi necessari per:

a) valutare se il terzo prestatore di servizi esegua le attività esternalizzate in maniera efficace e in conformità con i requisiti normativi e regolamentari applicabili e provveda a colmare adeguatamente le carenze riscontrate;

b) individuare i rischi che si pongono in relazione alle attività esternalizzate e effettuare un adeguato controllo periodico;

c) sottoporre le attività esternalizzate a procedure adeguate di controllo, anche in termini di effettiva vigilanza sulle attività e sui rischi associati nell'ambito dello stesso fornitore di servizi di comunicazione dati;

d) assicurare un'adeguata continuità operativa delle attività esternalizzate.

Ai fini della lettera d), il fornitore di servizi di comunicazione dati è informato delle disposizioni in materia di continuità operativa predisposte dal terzo prestatore di servizi, ne valuta la qualità e, se necessario, ne richiede miglioramenti.

5. Il fornitore di servizi di comunicazione dati provvede a che il terzo prestatore di servizi collabori con l'autorità competente del fornitore di servizi di comunicazione dati relativamente alle attività esternalizzate.

6. Il fornitore di servizi di comunicazione dati che esternalizza funzioni essenziali comunica all'autorità competente del proprio Stato membro d'origine:

a) l'identità del terzo prestatore di servizi;

b) i provvedimenti organizzativi e le politiche adottati in materia di esternalizzazione e i rischi che questa comporta secondo quanto indicato al paragrafo 4;

c) i rapporti interni o esterni sulle attività esternalizzate.

Ai fini del primo comma una funzione è considerata essenziale se un'anomalia nella sua esecuzione o la sua mancata esecuzione comprometterebbero gravemente la capacità del fornitore di servizi di comunicazione dati di continuare a garantire la conformità alle condizioni e agli obblighi dell'autorizzazione o agli altri obblighi imposti dalla direttiva 2014/65/UE.

Articolo 7

Continuità operativa e dispositivi di back-up

1. Il fornitore di servizi di comunicazione dati usa sistemi e dispositivi adeguati e sufficientemente solidi da assicurare la continuità e la regolarità della prestazione dei servizi previste alla direttiva 2014/65/UE.

2. Il fornitore di servizi di comunicazione dati esegue, a cadenza almeno annuale, riesami periodici delle infrastrutture tecniche impiegate e delle associate politiche e procedure, comprese le disposizioni in materia di continuità operativa. Il fornitore di servizi di comunicazione dati colma le carenze riscontrate in sede di riesame.

3. Il fornitore di servizi di comunicazione dati predispone efficaci disposizioni in materia di continuità operativa che gli permettano di affrontare gli eventi perturbatori, tra cui:

a) processi fondamentali per assicurare i servizi forniti, comprese le procedure di attivazione di livelli successivi di intervento, le attività esternalizzate interessate o la dipendenza da prestatori esterni;

b) disposizioni specifiche in materia di continuità operativa che coprano una gamma adeguata di scenari possibili, a breve e a medio termine, tra cui disfunzioni del sistema, calamità naturali, interruzione delle comunicazioni, perdita di personale essenziale e impossibilità di usare i locali in cui si svolge solitamente l'attività;

c) duplicazione delle componenti hardware in modo da attivare un meccanismo di subentro dell'infrastruttura di back-up, compresi la connettività di rete e i canali di comunicazione;

d) copie di sicurezza dei dati essenziali per l'attività e dei dati aggiornati dei contatti necessari, in modo da assicurare la comunicazione al suo interno e con la clientela;

e) procedure per trasferire e gestire i servizi di comunicazione dati da un sito di riserva;

f) tempo massimo prestabilito per il ripristino delle funzioni essenziali, che deve essere il più possibile breve e comunque non superiore a sei ore per i dispositivi di pubblicazione autorizzati (APA) e i fornitori di sistemi consolidati di pubblicazione (CTP) e non protrarsi oltre la fine del giorno lavorativo successivo per i meccanismi di segnalazione autorizzati (ARM);

g) formazione del personale sull'applicazione delle disposizioni in materia di continuità operativa e ruolo di ciascuno, compreso il personale preposto alle operazioni di sicurezza specificamente incaricato della reazione immediata all'interruzione del servizio.

4. Il fornitore di servizi di comunicazione dati predispone un programma di prove periodiche, riesame e, se necessario, modifica delle disposizioni in materia di continuità operativa.

5. Il fornitore di servizi di comunicazione dati segnala sul proprio sito web le eventuali interruzioni del servizio o perturbazioni nei collegamenti e ne informa immediatamente l'autorità competente del proprio Stato membro d'origine e i clienti, indicando il tempo stimato necessario per ripristinare la regolarità del servizio.

6. Nel caso degli ARM la notifica prevista al paragrafo 5 è trasmessa anche alle autorità competenti cui l'ARM presenta rendiconti delle operazioni.

Articolo 8

Prove e capacità

1. Il fornitore di servizi di comunicazione dati applica metodologie di sviluppo e di prova ben delineate che assicurino quanto segue:

a) il funzionamento dei sistemi informatici è conforme agli obblighi previsti dalla legge;

b) i controlli della conformità e della gestione dei rischi incorporati nei sistemi informatici funzionano come previsto;

c) i sistemi informatici sono in grado di continuare a funzionare in maniera efficace in qualsiasi momento.

2. Il fornitore di servizi di comunicazione dati applica le metodologie previste al paragrafo 1 anche prima e dopo ogni aggiornamento dei sistemi informatici.

3. Il fornitore di servizi di comunicazione dati notifica immediatamente all'autorità competente del proprio Stato membro d'origine qualsiasi modifica rilevante del sistema informatico programmata prima di apportarla.

4. Nel caso degli ARM la notifica prevista al paragrafo 3 è trasmessa anche alle autorità competenti cui l'ARM presenta rendiconti delle operazioni.

5. Il fornitore di servizi di comunicazione dati predispone un programma permanente di riesame periodico e, se necessario, di modifica delle metodologie di sviluppo e di prova.

6. Il fornitore di servizi di comunicazione dati effettua periodicamente prove di stress a cadenza almeno annuale. Il fornitore di servizi di comunicazione dati prevede nello scenario avverso impiegato nella prova di stress un comportamento inaspettato di elementi costitutivi essenziali dei sistemi e delle linee di comunicazione. La prova di stress verifica come l'hardware, il software e le comunicazioni reagiscono alle potenziali minacce e permette di individuare i sistemi incapaci di sopportare gli scenari avversi. Il fornitore di servizi di comunicazione dati adotta misure per colmare le carenze riscontrate nei sistemi.

7. Il fornitore di servizi di comunicazione dati:

a) dispone di capacità sufficiente per svolgere le sue funzioni senza disfunzioni o carenze, compreso sotto forma di dati mancanti o inesatti;

b) assicura una scalabilità sufficiente a assorbire senza indebito ritardo un aumento della mole di informazioni da elaborare e del numero di richieste di accesso da parte dei clienti.

Articolo 9

Sicurezza

1. Il fornitore di servizi di comunicazione dati predispone e mantiene procedure e disposizioni per la sicurezza fisica e elettronica intese a:

a) proteggere i sistemi informatici dall'uso improprio o dall'accesso non autorizzato;

b) ridurre al minimo i rischi di attacchi contro i sistemi di informazione quali definiti all'articolo 2, lettera a), della direttiva 2013/40/UE del Parlamento europeo e del Consiglio ([1]);

c) impedire la divulgazione non autorizzata di informazioni riservate;

d) garantire la sicurezza e l'integrità dei dati.

2. Per i casi in cui l'impresa di investimento («impresa segnalante») incarica un terzo («impresa trasmittente») di trasmettere per suo conto informazioni a un ARM, l'ARM predispone procedure e disposizioni che impediscono all'impresa trasmittente l'accesso a qualsiasi altra informazione sull'impresa segnalante o a qualsiasi altra informazione da questa trasmessa all'ARM in prima persona o per il tramite di un'altra impresa trasmittente.

3. Il fornitore di servizi di comunicazione dati predispone e mantiene misure e disposizioni per individuare immediatamente e gestire i rischi indicati al paragrafo 1.

4. Il fornitore di servizi di comunicazione dati notifica immediatamente le violazioni delle misure di sicurezza fisica e elettronica di cui ai paragrafi 1, 2 e 3:

a) all'autorità competente del proprio Stato membro d'origine, cui trasmette un rapporto sull'accaduto precisando la natura dell'evento, le misure adottate per farvi fronte e le iniziative prese per impedire il ripetersi di eventi simili;

b) ai clienti che subiscono le conseguenze della violazione della sicurezza.

([1]) Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

5. Nel caso degli ARM la notifica prevista al paragrafo 4, lettera a), è trasmessa anche alle autorità competenti cui l'ARM presenta rendiconti delle operazioni.

Articolo 10

Gestione delle informazioni incomplete o potenzialmente errate da parte degli APA e dei CTP

1. Gli APA e i CTP predispongono e mantengono disposizioni adeguate che permettono loro di pubblicare correttamente, senza introdurvi errori o omettere informazioni, i report delle operazioni concluse ricevuti dalle imprese di investimento e, per i CTP, dalle sedi di negoziazione e dagli APA e provvedono a correggere le informazioni nel caso in cui vi abbiano introdotto loro stessi errori o omissioni.

2. Gli APA e i CTP monitorano costantemente e in tempo reale le prestazioni dei loro sistemi informatici per accertare che la pubblicazione dei report delle operazioni concluse ricevuti sia andata a buon fine.

3. Gli APA e i CTP effettuano periodicamente una riconciliazione tra i report delle operazioni concluse ricevuti e quelli pubblicati per verificare se le informazioni sono state pubblicate correttamente.

4. L'APA conferma all'impresa di investimento segnalante di aver ricevuto il report delle operazioni concluse, indicando il codice identificativo che ha assegnato all'operazione. L'APA cita il codice identificativo dell'operazione in ogni successiva comunicazione con l'impresa segnalante relativa al corrispondente report delle operazioni concluse.

5. L'APA predispone e mantiene dispositivi adeguati per individuare all'arrivo i report delle operazioni concluse incompleti o contenenti informazioni probabilmente errate. Detti dispositivi comportano allarmi automatici su prezzo e volume, tenuto conto di quanto segue:

a) settore e segmento in cui è negoziato lo strumento finanziario;

b) livelli di liquidità, compresi i livelli storici di negoziazione;

c) parametri di riferimento adeguati su prezzo e volume;

d) se necessario, altri parametri consoni alle caratteristiche dello strumento finanziario.

6. Se il report dell'operazione conclusa ricevuto risulta incompleto o contiene informazioni probabilmente errate, l'APA non lo pubblica e avvisa immediatamente l'impresa d'investimento che lo ha trasmesso.

7. In situazioni eccezionali gli APA e i CTP cancellano o modificano informazioni contenute nei report delle operazioni concluse, su richiesta del soggetto che le ha fornite, laddove motivi tecnici impediscano a tale soggetto di cancellarle o modificarle direttamente.

8. Gli APA rendono pubbliche le politiche non discriminatorie applicate alla cancellazione e alla modifica delle informazioni contenute nei report delle operazioni concluse, indicando le sanzioni in cui l'impresa di investimento che ha trasmesso il report può incorrere qualora le informazioni incomplete o errate abbiano determinato la cancellazione o la modifica del report.

Articolo 11

Gestione delle informazioni incomplete o potenzialmente errate da parte degli ARM

1. L'ARM predispone e mantiene dispositivi adeguati per individuare i rendiconti delle operazioni incompleti o contenenti errori evidenti attribuibili al cliente. L'ARM convalida i rendiconti delle operazioni per il campo, il formato e il contenuto dei campi a fronte dei requisiti stabiliti dall'articolo 26 del regolamento (UE) n. 600/2014, conformemente all'allegato I, tabella 1 del regolamento delegato (UE) 2017/590 della Commissione ([1]).

([1]) Regolamento delegato (UE) 2017/590 della Commissione, del 28 luglio 2016, che integra il regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione relative alla segnalazione delle operazioni alle autorità competenti (cfr. pag. 449 della presente Gazzetta ufficiale).

2. L'ARM predispone e mantiene dispositivi adeguati per individuare i rendiconti delle operazioni che contengono errori o omissioni da esso stesso causati e per correggerli, anche mediante cancellazione o modifica. L'ARM esegue la convalida per il campo, il formato e il contenuto dei campi conformemente all'allegato I, tabella 1 del regolamento delegato (UE) 2017/590.

3. L'ARM monitora costantemente e in tempo reale le prestazioni dei propri sistemi per accertare che il rendiconto delle operazioni ricevuto sia segnalato correttamente all'autorità competente conformemente all'articolo 26 del regolamento (UE) n. 600/2014.

4. Su richiesta dell'autorità competente del proprio Stato membro d'origine o dell'autorità competente cui trasmette i rendiconti delle operazioni, l'ARM effettua periodicamente una riconciliazione tra le informazioni ricevute dal cliente o generate per conto del cliente a fini di segnalazione delle operazioni e i campioni di dati forniti dall'autorità competente.

5. Se non sono finalizzate a correggere errori o omissioni attribuibili all'ARM, le correzioni, comprese la cancellazione o modifica dei rendiconti delle operazioni, sono possibili soltanto su richiesta del cliente e per un rendiconto alla volta. Se cancella o modifica il rendiconto di un'operazione su richiesta del cliente, l'ARM gli trasmette il risultante rendiconto aggiornato.

6. Se prima di trasmettere il rendiconto dell'operazione riscontra un errore o un'omissione attribuibile al cliente, l'ARM non trasmette il rendiconto e notifica immediatamente all'impresa di investimento i particolari dell'errore o dell'omissione in modo da consentire al cliente di presentare informazioni corrette.

7. Laddove riscontri di aver introdotto un errore o omissione nel rendiconto, l'ARM ne presenta immediatamente una versione corretta e completa.

8. L'ARM notifica immediatamente al cliente i particolari dell'errore o dell'omissione e gli trasmette il rendiconto dell'operazione aggiornato. L'ARM notifica immediatamente l'errore o l'omissione anche all'autorità competente del proprio Stato membro d'origine e all'autorità competente cui ha segnalato il rendiconto dell'operazione.

9. L'obbligo di correggere o cancellare i rendiconti delle operazioni errati ovvero di segnalare le operazioni omesse non si applica agli errori o omissioni compiuti oltre cinque anni prima della data in cui l'ARM ne è venuto a conoscenza.

Articolo 12

Connettività degli ARM

1. L'ARM predispone le politiche, i dispositivi e le capacità tecniche necessari per conformarsi alle specifiche tecniche relative alla presentazione dei rendiconti delle operazioni prescritte dall'autorità competente del proprio Stato membro d'origine e dalle altre autorità competenti cui trasmette rendiconti delle operazioni.

2. L'ARM predispone le politiche, i dispositivi e le capacità tecniche adeguati per poter ricevere dai clienti i rendiconti delle operazioni e ritrasmettere loro le informazioni. L'ARM fornisce al cliente copia del rendiconto delle operazioni che ha presentato per suo conto all'autorità competente.

Articolo 13

Altri servizi prestati dai CTP

1. Il CTP può prestare gli ulteriori servizi seguenti:

a) fornitura di dati sulla trasparenza pre-negoziazione;

b) fornitura di dati storici;

c) fornitura di dati di riferimento;

d) fornitura di servizi di ricerca;

e) elaborazione, distribuzione e commercializzazione di dati e statistiche sugli strumenti finanziari e le sedi di negoziazione e altri dati di mercato;

f) progettazione, gestione, manutenzione e commercializzazione di hardware, software e reti per la trasmissione di dati e informazioni.

2. Oltre ai servizi citati al paragrafo 1 il CTP può prestare altri servizi di miglioramento dell'efficienza del mercato, a condizione che non espongano la qualità del sistema consolidato di pubblicazione o l'indipendenza del CTP a rischi impossibili da prevenire o attenuare adeguatamente.

CAPO III

DISPOSITIVI DI PUBBLICAZIONE

(Articolo 64, paragrafi 1 e 2, e articolo 65, paragrafo 1, della direttiva 2014/65/UE)

Articolo 14

Pubblicazione in linguaggio macchina

1. Gli APA e i CTP pubblicano in linguaggio macchina le informazioni di cui l'articolo 64, paragrafo 1, e l'articolo 65, paragrafo 1, della direttiva 2014/65/UE prescrivono la pubblicazione.

2. I CTP pubblicano in linguaggio macchina le informazioni previste dall'articolo 65, paragrafo 2, della direttiva 2014/65/UE.

3. Sono considerate pubblicate in linguaggio macchina soltanto le informazioni che soddisfano tutte le condizioni seguenti:

a) sono in un formato elettronico atto a essere letto direttamente e automaticamente da un computer;

b) sono conservate in un'architettura informatica conforme all'articolo 8, paragrafo 7, che consente l'accesso automatico;

c) sono gestite da un sistema sufficientemente solido da assicurare la continuità e la regolarità dei servizi prestati e tale da permettere una velocità di accesso adeguata;

d) sono accessibili, leggibili, utilizzabili e copiabili da un software informatico disponibile pubblicamente e gratuitamente.

Ai fini del primo comma, lettera a), il formato elettronico è determinato da standard aperti, gratuiti e non proprietari.

4. Ai fini del paragrafo 3, primo comma, lettera a), il formato elettronico indica il tipo di file o messaggi, le regole che li identificano e il nome e tipo di dati dei campi previsti.

5. Gli APA e i CTP:

a) mettono a disposizione del pubblico istruzioni sul modo e il luogo in cui è possibile accedere agevolmente ai dati e usarli, indicando anche il formato elettronico;

b) rendono note le modifiche delle istruzioni di cui alla lettera a) almeno tre mesi prima della loro entrata in vigore, salvo in caso di necessità urgente e debitamente motivata di una loro entrata in vigore in tempi più rapidi;

c) inseriscono nella pagina iniziale del proprio sito web un collegamento ipertestuale alle istruzioni di cui alla lettera a).

Articolo 15

Ambito del sistema consolidato di pubblicazione per azioni, certificati di deposito, fondi indicizzati quotati, certificati e altri strumenti finanziari analoghi

1. Il CTP include nel flusso di dati elettronici i dati resi pubblici a norma degli articoli 6 e 20 del regolamento (UE) n. 600/2014 relativamente a tutti gli strumenti finanziari di cui a detti articoli.

2. Quando un nuovo APA o una nuova sede di negoziazione iniziano l'attività, il CTP include i dati da questi resi pubblici nel flusso dei dati elettronici del proprio sistema consolidato di pubblicazione in tempi il più possibile brevi e comunque non oltre sei mesi dopo l'inizio dell'attività dell'APA o della sede di negoziazione.

Articolo 16

Distinzione fra report delle operazioni concluse originali e duplicati per azioni, certificati di deposito, fondi indicizzati quotati, certificati e altri strumenti finanziari analoghi

1. Quando pubblica un report delle operazioni concluse che è un duplicato, l'APA inserisce il codice «DUPL» nel campo della ristampa per consentire ai destinatari dei dati di distinguere il report originale dai duplicati.

2. Ai fini del paragrafo 1 l'APA impone a ciascuna impresa di investimento di soddisfare una delle condizioni seguenti:

a) certificare che segnala le operazioni su un dato strumento finanziario soltanto per il tramite dell'APA stesso;

b) applicare un meccanismo di identificazione che, per una data operazione, contrassegna un report come originale («ORGN») e tutti gli altri come duplicati («DUPL»).

Articolo 17

Pubblicazione dei report originali per azioni, certificati di deposito, fondi indicizzati quotati, certificati e altri strumenti finanziari analoghi

Il CTP non consolida i report delle operazioni concluse contrassegnati dal codice «DUPL» nel campo della ristampa.

Articolo 18

Informazioni che l'APA è tenuto a pubblicare

1. L'APA pubblica:

a) per le operazioni eseguite su azioni, certificati di deposito, fondi indicizzati quotati, certificati e altri strumenti finanziari analoghi, le informazioni specificate nell'allegato I, tabella 2, del regolamento delegato (UE) 2017/587, indicando i contrassegni appropriati elencati nell'allegato I, tabella 3, del regolamento delegato (UE) 2017/587;

b) per le operazioni eseguite su obbligazioni, strumenti finanziari strutturati, quote di emissione e strumenti derivati, le informazioni specificate nell'allegato II, tabella 1, del regolamento delegato (UE) 2017/583, indicando i contrassegni appropriati elencati nell'allegato II, tabella 2, del regolamento delegato (UE) 2017/583.

2. Ai fini della pubblicazione delle informazioni sul momento in cui è stata segnalata l'operazione, l'APA indica la data e l'ora, specificata fino ai minuti secondi, in cui ha pubblicato l'operazione.

3. In deroga al paragrafo 2, l'APA che pubblica informazioni su un'operazione eseguita in un sistema elettronico indica la data e l'ora, specificata fino al millisecondo, della pubblicazione dell'operazione nel suo report delle operazioni concluse.

4. Ai fini del paragrafo 3, per «sistema elettronico» s'intende un sistema in cui gli ordini sono negoziabili per via elettronica oppure sono negoziabili al di fuori del sistema ma pubblicizzati attraverso il sistema.

5. Le marche temporali previste ai paragrafi 2 e 3 non si discostano, rispettivamente, di più di un secondo o di un millisecondo dal tempo universale coordinato (UTC) emanato e mantenuto da uno dei centri di metrologia del tempo elencati nell'ultima relazione di attività sul tempo del Bureau International des Poids et Mesures (BIPM).

Articolo 19

Non discriminazione

Gli APA e i CTP provvedono a che le informazioni da rendere pubbliche siano trasmesse contemporaneamente su tutti i canali di distribuzione, anche quando sono rese pubbliche per quanto tecnicamente possibile in tempo reale o 15 minuti dopo la prima pubblicazione.

Articolo 20

Informazioni che i CTP sono tenuti a pubblicare

Il CTP pubblica:

(a) per le operazioni eseguite su azioni, certificati di deposito, fondi indicizzati quotati, certificati e altri strumenti finanziari analoghi, le informazioni specificate nell'allegato I, tabella 2, del regolamento delegato (UE) 2017/587 indicando i contrassegni appropriati elencati nell'allegato I, tabella 3, del regolamento delegato (UE) 2017/587;

(b) per le operazioni eseguite su obbligazioni, strumenti finanziari strutturati, quote di emissione e strumenti derivati, le informazioni specificate nell'allegato II, tabella 1, del regolamento delegato (UE) 2017/583 indicando i contrassegni appropriati elencati nell'allegato II, tabella 2, del regolamento delegato (UE) 2017/583.

Articolo 21

Entrata in vigore e applicazione

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Esso si applica a decorrere dalla prima data che figura all'articolo 93, paragrafo 1, secondo comma, della direttiva 2014/65/UE.

Tuttavia, l'articolo 14, paragrafo 2, e l'articolo 20, lettera b), si applicano a decorrere dal primo giorno del nono mese successivo alla data di applicazione della direttiva 2014/65/UE.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 2 giugno 2016

Per la Commissione

Il presidente

Jean-Claude JUNCKER