

**DECISIONE DELLA COMMISSIONE****del 4 maggio 2010****relativa al piano di sicurezza per il funzionamento del sistema di informazione visti**

(2010/260/UE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS) <sup>(1)</sup>, in particolare l'articolo 32,

considerando quanto segue:

- (1) Ai sensi dell'articolo 32, paragrafo 3, del regolamento (CE) n. 767/2008, l'Autorità di gestione adotta le misure necessarie per conseguire gli obiettivi in materia di sicurezza enunciati all'articolo 32, paragrafo 2, per quanto riguarda il funzionamento del VIS, compresa l'adozione di un piano di sicurezza.
- (2) Ai sensi dell'articolo 26, paragrafo 4, del regolamento (CE) n. 767/2008, durante un periodo transitorio, prima che l'Autorità di gestione entri in funzione, la Commissione è responsabile della gestione operativa del VIS.
- (3) Al trattamento dei dati personali effettuato dalla Commissione nell'espletamento dei suoi compiti di responsabile della gestione operativa del VIS si applica il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio <sup>(2)</sup>.
- (4) Ai sensi dell'articolo 26, paragrafo 7, del regolamento (CE) n. 767/2008, la Commissione, qualora deleghi la propria responsabilità durante il periodo transitorio prima che l'Autorità di gestione entri in funzione, assicura che tale delega non si ripercuota negativamente sull'efficacia dei meccanismi di controllo previsti dal diritto dell'Unione, siano essi a cura della Corte di giustizia, della Corte dei conti o del garante europeo della protezione dei dati.
- (5) Una volta entrata in funzione, l'Autorità di gestione deve stabilire il proprio piano di sicurezza in relazione al VIS.
- (6) La decisione 2008/602/CE della Commissione, del 17 giugno 2008, che stabilisce l'architettura fisica e i

requisiti delle interfacce nazionali e dell'infrastruttura di comunicazione fra il VIS centrale e le interfacce nazionali nella fase di sviluppo <sup>(3)</sup> descrive i servizi di sicurezza richiesti per la rete VIS.

- (7) Ai sensi dell'articolo 27 del regolamento (CE) n. 767/2008, il VIS centrale principale, che svolge funzioni di controllo e gestione tecnici, ha sede a Strasburgo (Francia), mentre il VIS centrale di riserva, in grado di assicurare tutte le funzioni del VIS centrale principale in caso di guasto del sistema, si trova a Sankt Johann im Pongau (Austria).
- (8) Occorre definire i ruoli dei responsabili della sicurezza al fine di garantire una risposta efficace e rapida agli incidenti di sicurezza e il relativo rapporto.
- (9) Deve essere stabilita una politica di sicurezza che descriva tutti gli aspetti tecnici e organizzativi in conformità delle disposizioni della presente decisione.
- (10) È necessario definire misure che garantiscano un livello di sicurezza adeguato per il funzionamento del VIS,

HA ADOTTATO LA PRESENTE DECISIONE:

## CAPO I

**DISPOSIZIONI GENERALI***Articolo 1***Oggetto**

La presente decisione stabilisce l'organizzazione e le misure di sicurezza (piano di sicurezza) ai sensi dell'articolo 32, paragrafo 3, del regolamento (CE) n. 767/2008.

## CAPO II

**ORGANIZZAZIONE, RESPONSABILITÀ E GESTIONE DEGLI INCIDENTI***Articolo 2***Compiti della Commissione**

1. La Commissione attua le misure di sicurezza per il VIS centrale e l'infrastruttura di comunicazione di cui alla presente decisione, e ne controlla l'efficacia.

<sup>(1)</sup> GU L 218 del 13.8.2008, pag. 60.

<sup>(2)</sup> GU L 8 del 12.1.2001, pag. 1.

<sup>(3)</sup> GU L 194 del 23.7.2008, pag. 3.

2. La Commissione designa tra i suoi funzionari un responsabile della sicurezza del sistema. Il responsabile della sicurezza del sistema è nominato dal direttore generale della direzione generale «Giustizia, libertà e sicurezza» della Commissione, ed esegue in particolare i seguenti compiti:

- a) elabora, aggiorna e rivede la politica di sicurezza di cui all'articolo 7 della presente decisione;
- b) controlla l'efficacia dell'attuazione delle procedure di sicurezza per il VIS centrale e l'infrastruttura di comunicazione;
- c) contribuisce all'elaborazione delle relazioni in materia di sicurezza previste dall'articolo 50, paragrafi 3 e 4, del regolamento (CE) n. 767/2008;
- d) svolge compiti di coordinamento e presta assistenza nell'ambito dei controlli effettuati dal garante europeo della protezione dei dati ai sensi dell'articolo 42 del regolamento (CE) n. 767/2008;
- e) controlla che tutti gli appaltatori e subappaltatori comunque associati alla gestione e al funzionamento del VIS applichino correttamente e integralmente la presente decisione e la politica di sicurezza;
- f) f) tiene un elenco dei punti di contatto nazionali unici per la sicurezza del VIS e lo trasmette ai responsabili locali della sicurezza del VIS centrale e dell'infrastruttura di comunicazione.

### Articolo 3

#### Responsabile locale della sicurezza del VIS centrale

1. Fatto salvo l'articolo 8, la Commissione designa tra i suoi funzionari un responsabile locale della sicurezza del VIS centrale. Vanno evitati i conflitti d'interesse tra l'incarico di responsabile locale della sicurezza e altro incarico ufficiale. Nomina il responsabile locale della sicurezza del VIS centrale il direttore generale della direzione generale «Giustizia, libertà e sicurezza» della Commissione.

2. Il responsabile locale della sicurezza del VIS centrale garantisce l'attuazione delle misure di sicurezza di cui alla presente decisione e l'osservanza delle procedure di sicurezza nel VIS centrale principale. Per quanto riguarda il VIS centrale di riserva, il responsabile locale della sicurezza del VIS centrale garantisce l'attuazione delle misure di sicurezza di cui alla presente decisione, escluse quelle previste dall'articolo 10, e l'osservanza delle procedure di sicurezza connesse.

3. Il responsabile locale della sicurezza del VIS centrale può delegare a personale subalterno i compiti assegnatigli. Vanno

evitati i conflitti d'interesse tra l'incarico di eseguire tali compiti e altro incarico ufficiale. Un numero telefonico unico e un indirizzo unico permettono di raggiungere in qualsiasi momento il responsabile locale della sicurezza o il suo subalterno.

4. Nei limiti di cui al paragrafo 1, il responsabile locale della sicurezza del VIS centrale esegue i compiti derivanti dalle misure di sicurezza da prendere locali in cui sono ubicati il VIS centrale principale e il VIS centrale di riserva, e in particolare:

- a) svolge compiti di sicurezza operativa locale comprendenti il controllo dei firewall, test periodici di sicurezza, controlli e rapporti;
- b) controlla l'efficacia del piano di continuità operativa e garantisce lo svolgimento di esercitazioni periodiche;
- c) raccoglie prove sugli incidenti che possono avere ripercussioni sulla sicurezza del VIS centrale o dell'infrastruttura di comunicazione, e ne riferisce al responsabile della sicurezza del sistema;
- d) informa il responsabile della sicurezza del sistema quando occorre modificare la politica di sicurezza;
- e) controlla che tutti gli appaltatori e subappaltatori comunque associati alla gestione e al funzionamento del VIS applichino la presente decisione e la politica di sicurezza;
- f) garantisce che i membri del personale siano a conoscenza dei loro obblighi e controlla l'applicazione della politica di sicurezza;
- g) controlla gli sviluppi in materia di sicurezza informatica e provvede affinché i membri del personale ricevano una formazione adeguata;
- h) prepara le informazioni di base e le opzioni necessarie per elaborare, aggiornare e rivedere la politica di sicurezza in conformità dell'articolo 7.

### Articolo 4

#### Responsabile locale della sicurezza dell'infrastruttura di comunicazione

1. Fatto salvo l'articolo 8, la Commissione designa tra i suoi funzionari un responsabile locale della sicurezza dell'infrastruttura di comunicazione. Vanno evitati i conflitti d'interesse tra l'incarico di responsabile locale della sicurezza e altro incarico ufficiale. Nomina il responsabile locale della sicurezza dell'infrastruttura di comunicazione il direttore generale della direzione generale «Giustizia, libertà e sicurezza» della Commissione.

2. Il responsabile locale della sicurezza dell'infrastruttura di comunicazione controlla il funzionamento dell'infrastruttura di comunicazione e garantisce l'attuazione delle misure di sicurezza e l'osservanza delle procedure di sicurezza.

3. Il responsabile locale della sicurezza dell'infrastruttura di comunicazione può delegare a personale subalterno i compiti assegnatigli. Vanno evitati i conflitti d'interesse tra l'incarico di eseguire tali compiti e altro incarico ufficiale. Un numero telefonico unico e un indirizzo unico permettono di raggiungere in qualsiasi momento il responsabile locale della sicurezza o il suo subalterno.

4. Il responsabile locale della sicurezza dell'infrastruttura di comunicazione esegue i compiti derivanti dalle misure di sicurezza relative all'infrastruttura di comunicazione, e in particolare:

- a) svolge tutti i compiti di sicurezza operativa connessi all'infrastruttura di comunicazione comprendenti il controllo dei firewall, test periodici di sicurezza, controlli e rapporti;
- b) controlla l'efficacia del piano di continuità operativa e garantisce lo svolgimento di esercitazioni periodiche;
- c) raccoglie prove sugli incidenti che possono avere ripercussioni sulla sicurezza dell'infrastruttura di comunicazione o del VIS centrale o sui sistemi nazionali, e ne riferisce al responsabile della sicurezza del sistema;
- d) informa il responsabile della sicurezza del sistema quando occorre modificare la politica di sicurezza;
- e) controlla che tutti gli appaltatori e subappaltatori comunque associati alla gestione dell'infrastruttura di comunicazione applichino la presente decisione e la politica di sicurezza;
- f) garantisce che i membri del personale siano a conoscenza dei loro obblighi e controlla l'applicazione della politica di sicurezza;
- g) controlla gli sviluppi in materia di sicurezza informatica e provvede affinché i membri del personale ricevano una formazione adeguata;
- h) prepara le informazioni di base e le opzioni necessarie per elaborare, aggiornare e rivedere la politica di sicurezza in conformità dell'articolo 7.

## Articolo 5

### Incidenti di sicurezza

1. È considerato incidente di sicurezza qualunque evento che ha o può avere ripercussioni sulla sicurezza del funzionamento del VIS e può causare danni o perdite al VIS, in particolare quando possono essere stati consultati dati senza autorizzazione o quando sono state o possono essere state compromesse la disponibilità, l'integrità e la riservatezza dei dati.

2. La politica di sicurezza stabilisce procedure di ripristino in caso di incidente. Gli incidenti di sicurezza sono gestiti in modo da garantire una risposta rapida, efficace e corretta conformemente alla politica di sicurezza.

3. Le informazioni relative a un incidente di sicurezza che ha o può avere ripercussioni sul funzionamento del VIS in uno Stato membro o sulla disponibilità, sull'integrità e sulla riservatezza dei dati VIS inseriti da uno Stato membro sono trasmesse allo Stato membro interessato. Gli incidenti di sicurezza sono notificati al responsabile della protezione dei dati della Commissione.

## Articolo 6

### Gestione degli incidenti

1. Tutti i membri del personale e gli appaltatori associati allo sviluppo, alla gestione o al funzionamento del VIS sono tenuti a prendere nota di qualunque carenza di sicurezza, rilevata o presunta, nel funzionamento del VIS e a riferirne al responsabile della sicurezza del sistema o al responsabile locale della sicurezza del VIS centrale ovvero al responsabile locale della sicurezza dell'infrastruttura di comunicazione, a seconda dei casi.

2. Qualora sia individuato un incidente che ha o può avere ripercussioni sulla sicurezza del funzionamento del VIS, il responsabile locale della sicurezza del VIS centrale o il responsabile locale della sicurezza dell'infrastruttura di comunicazione ne informa il più rapidamente possibile il responsabile della sicurezza del sistema e, se del caso, il punto di contatto nazionale unico per la sicurezza del VIS eventualmente esistente nello Stato membro in questione, per iscritto o, in caso di estrema urgenza, con altro mezzo di comunicazione. Nel rapporto è descritto l'incidente di sicurezza e sono indicati il livello di rischio, le possibili conseguenze e le misure prese o da prendere per attenuare il rischio.

3. Il responsabile locale della sicurezza del VIS centrale o, a seconda dei casi, il responsabile locale della sicurezza dell'infrastruttura di comunicazione raccolgono immediatamente tutte le prove relative all'incidente di sicurezza. Nei limiti delle disposizioni applicabili in materia di protezione dei dati, tali prove sono messe a disposizione del responsabile della sicurezza del sistema, su sua istanza.

4. Sono messe in atto procedure di feedback per assicurare che, una volta affrontato e risolto l'incidente di sicurezza, ne siano notificati i risultati.

## CAPO III

**MISURE DI SICUREZZA***Articolo 7***Politica di sicurezza**

1. Il direttore generale della direzione generale «Giustizia, libertà e sicurezza» elabora, aggiorna e rivede periodicamente una politica di sicurezza vincolante in conformità della presente decisione. La politica di sicurezza precisa le procedure e le misure di protezione dalle minacce dirette alla disponibilità, all'integrità e alla riservatezza del VIS, compreso un piano di emergenza, al fine di garantire il livello di sicurezza adeguato previsto dalla presente decisione. La politica di sicurezza è conforme alla presente decisione.

2. La politica di sicurezza si basa su una valutazione dei rischi. Le misure descritte dalla politica di sicurezza sono proporzionate ai rischi individuati.

3. La valutazione dei rischi e la politica di sicurezza sono aggiornate se innovazioni tecnologiche, l'individuazione di nuove minacce o altre circostanze lo rendono necessario. In ogni caso la politica di sicurezza è rivista annualmente per garantirne la continua rispondenza all'ultima valutazione dei rischi o ad altre eventuali innovazioni tecnologiche, minacce o circostanze pertinenti.

4. La politica di sicurezza è elaborata dal responsabile della sicurezza del sistema in collaborazione con il responsabile locale della sicurezza del VIS e il responsabile locale della sicurezza dell'infrastruttura di comunicazione.

*Articolo 8***Attuazione delle misure di sicurezza**

1. È possibile affidare a enti pubblici o privati l'esecuzione dei compiti e l'attuazione dei requisiti previsti dalla presente decisione e dalla politica di sicurezza, compreso il compito di designare il responsabile locale della sicurezza.

2. In tal caso la Commissione provvede con un accordo giuridicamente vincolante affinché sia garantito il pieno rispetto dei requisiti previsti dalla presente decisione e dalla politica di sicurezza. Qualora sia delegata o data in appalto la designazione del responsabile locale della sicurezza, la Commissione si assicura con un accordo giuridicamente vincolante di essere consultata sulla persona da designare per tale incarico.

*Articolo 9***Controlli all'ingresso delle installazioni**

1. Al fine di proteggere le zone che ospitano strutture di elaborazione dati sono usati perimetri di sicurezza muniti di adeguate barriere e di controlli alle entrate.

2. All'interno dei perimetri di sicurezza sono create zone sicure per proteggere i componenti fisici (attivi), compresi hardware, supporti di dati e console, piani e altri documenti sul VIS, gli uffici e le altre postazioni di lavoro del personale associato al funzionamento del VIS. Le zone sicure sono protette da adeguati controlli alle entrate per garantire l'accesso esclusivamente al personale autorizzato. Nelle zone sicure, il lavoro è soggetto alle dettagliate norme di sicurezza previste dalla politica di sicurezza.

3. Sono predisposti e installati dispositivi per garantire la sicurezza fisica degli uffici, dei locali e delle installazioni. Per evitare l'accesso non autorizzato, sono controllati e se possibile isolati dalle installazioni informatiche i punti d'accesso come le zone di consegna e di carico e altri punti da cui potrebbero entrare nei locali persone non autorizzate.

4. È messa a punto una protezione fisica del perimetro di sicurezza contro i danni da calamità naturali o provocate dall'uomo, da applicarsi in proporzione al rischio.

5. Le apparecchiature sono protette dalle minacce fisiche e ambientali e dal rischio di accesso non autorizzato.

6. Se dispone dell'informazione, la Commissione aggiunge all'elenco di cui all'articolo 2, paragrafo 2, lettera f), un punto di contatto unico per il controllo dell'attuazione delle disposizioni del presente articolo nei locali in cui è ubicato il VIS centrale di riserva.

*Articolo 10***Supporti di dati e controllo degli attivi**

1. I supporti rimovibili contenenti i dati sono protetti dall'accesso non autorizzato, dall'uso improprio o dalla corruzione, e la loro leggibilità è assicurata per tutto il ciclo di vita dei dati.

2. Quando non sono più utili i supporti vengono gettati in modo sicuro secondo le dettagliate procedure di sicurezza previste dalla politica di sicurezza.

3. Sono creati inventari per garantire la disponibilità di informazioni sui luoghi di conservazione, sul periodo di conservazione applicabile e sulle autorizzazioni di accesso.

4. Tutti gli attivi importanti del VIS centrale e dell'infrastruttura di comunicazione sono identificati in modo da poterli proteggere a seconda della loro rilevanza. È tenuto un inventario aggiornato delle apparecchiature TI pertinenti.

5. È messa a disposizione una documentazione aggiornata sul VIS centrale e sull'infrastruttura di comunicazione. Tale documentazione deve essere protetta dall'accesso non autorizzato.

*Articolo 11***Controllo della conservazione**

1. Sono prese misure adeguate per garantire la corretta conservazione dei dati e la loro protezione dall'accesso non autorizzato.

2. Tutte le apparecchiature contenenti supporti di conservazione sono controllate prima di essere gettate per garantire che i dati sensibili siano stati rimossi o integralmente sovrascritti, oppure sono distrutte in modo sicuro.

*Articolo 12***Controllo delle password**

1. Tutte le password sono conservate in modo sicuro e trattate come riservate. Qualora si sospetti che una password sia stata divulgata, questa è cambiata immediatamente o l'account utente è disattivato. Sono usate identità di utente individuali e uniche.

2. La politica di sicurezza definisce le procedure di connessione e disconnessione in modo da prevenire l'accesso non autorizzato.

*Articolo 13***Controllo dell'accesso**

1. La politica di sicurezza fissa la procedura formale di registrazione e deregistrazione del personale per la concessione e la revoca del diritto di accesso all'hardware e al software del VIS presso il sito del VIS centrale ai fini della gestione operativa. L'attribuzione e l'uso di adeguate credenziali di accesso (password o altri mezzi idonei) sono controllati con la procedura di gestione formale stabilita dalla politica di sicurezza.

2. L'accesso all'hardware e al software del VIS presso il sito del VIS centrale:

- i) è limitato alle persone autorizzate;
- ii) è limitato ai casi in cui può essere individuato uno scopo legittimo ai sensi dell'articolo 42 e dell'articolo 50, paragrafo 2, del regolamento (CE) n. 767/2008;
- iii) non eccede la durata e la portata necessarie per il suo scopo,  
e
- iv) è effettuato secondo una politica di controllo dell'accesso definita dalla politica di sicurezza.

3. Presso il VIS centrale sono usati solo i software e le console autorizzati dal responsabile locale della sicurezza del VIS

centrale. L'uso di funzioni di sistema che potrebbero scavalcare i controlli di sistema e delle applicazioni è limitato e controllato. Sono istituite procedure per controllare l'installazione dei software.

*Articolo 14***Controllo della comunicazione**

L'infrastruttura di comunicazione è soggetta a controlli volti a garantire la disponibilità, l'integrità e la riservatezza degli scambi di informazioni. Per proteggere i dati trasmessi nell'infrastruttura di comunicazione sono usati strumenti crittografici.

*Articolo 15***Controllo della registrazione dei dati**

Il responsabile locale della sicurezza del VIS centrale controlla gli account delle persone autorizzate ad accedere al software VIS dal VIS centrale. L'uso di tali account, compresa la data e l'ora e l'identità utente, è registrato.

*Articolo 16***Controllo del trasporto**

1. La politica di sicurezza definisce misure adeguate per impedire che i dati personali siano letti, copiati, modificati o cancellati senza autorizzazione durante la loro trasmissione dal VIS o verso il medesimo ovvero durante il trasporto dei supporti di dati. La politica di sicurezza contiene disposizioni in ordine ai tipi di invio o trasporto ammissibili e alle procedure sulla responsabilità del trasporto di elementi e del loro arrivo a destinazione. I supporti di dati non contengono dati diversi da quelli da inviare.

2. I servizi forniti da terzi che implicano l'accesso a dati, la loro elaborazione e comunicazione, la gestione di strutture di elaborazione dati o l'aggiunta di prodotti o servizi a tali strutture sono oggetto di controlli di sicurezza integrati e adeguati.

*Articolo 17***Sicurezza dell'infrastruttura di comunicazione**

1. L'infrastruttura di comunicazione è gestita e controllata in modo che risulti protetta dalle minacce e che sia garantita la sua sicurezza e quella del VIS centrale, compresi i dati scambiati suo tramite.

2. Nell'accordo di servizi di rete concluso con il fornitore di servizi sono indicati i requisiti di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete.

3. Oltre ai punti di accesso al VIS sono protetti tutti i servizi addizionali usati dall'infrastruttura di comunicazione. A tal fine la politica di sicurezza definisce misure adeguate.

*Articolo 18***Monitoraggio**

1. I registri (log) delle informazioni di cui all'articolo 34, paragrafo 1, del regolamento (CE) n. 767/2008 relative ad ogni accesso al VIS centrale e a tutte le operazioni di trattamento dei dati nell'ambito del VIS centrale sono conservati in modo sicuro e sono accessibili dai locali in cui si trovano il VIS centrale principale e il VIS centrale di riserva per il periodo previsto all'articolo 34, paragrafo 2, del regolamento (CE) n. 767/2008.

2. La politica di sicurezza fissa le procedure di monitoraggio dell'uso o dei guasti delle strutture di elaborazione dati e i risultati del monitoraggio sono rivisti periodicamente. Se necessario sono prese misure adeguate.

3. I dispositivi di registrazione e i registri sono protetti da manomissioni e dall'accesso non autorizzato in modo da rispondere ai requisiti di raccolta e conservazione per il periodo di conservazione dei dati.

*Articolo 19***Cifratura**

Ove opportuno sono usati strumenti crittografici per proteggere le informazioni. Il loro uso, le finalità e le condizioni devono ricevere l'approvazione preventiva del responsabile della sicurezza del sistema.

## CAPO IV

**SICUREZZA DELLE RISORSE UMANE***Articolo 20***Profili personali**

1. La politica di sicurezza descrive le funzioni e le responsabilità delle persone autorizzate ad accedere al VIS e all'infrastruttura di comunicazione.

2. I ruoli e le responsabilità in materia di sicurezza del personale della Commissione, degli appaltatori e del personale associato alla gestione operativa sono definiti, documentati e comunicati agli interessati. La descrizione delle mansioni e degli obiettivi precisa i ruoli e le responsabilità del personale della Commissione; i ruoli e le responsabilità degli appaltatori sono fissati nei contratti o negli accordi sul livello di servizio.

3. Sono conclusi accordi in materia di segretezza e riservatezza con tutte le persone cui non si applicano le norme sul servizio pubblico dell'Unione europea o di uno Stato membro. I membri del personale che devono lavorare con i dati VIS dispongono della necessaria autorizzazione o certificazione di sicurezza secondo le dettagliate procedure di sicurezza previste dalla politica di sicurezza.

*Articolo 21***Informazione del personale**

1. Tutti i membri del personale e, se del caso, gli appaltatori ricevono una formazione adeguata in materia di sensibilizzazione alla sicurezza, requisiti giuridici, politiche e procedure, nella misura necessaria all'esercizio delle loro funzioni.

2. Riguardo alla cessazione del rapporto di lavoro o del contratto, la politica di sicurezza definisce le responsabilità dei membri del personale e degli appaltatori in relazione al cambiamento di funzioni o alla cessazione del rapporto di lavoro, nonché le procedure per la restituzione degli attivi e la revoca dei diritti di accesso.

## CAPO V

**DISPOSIZIONI FINALI***Articolo 22***Applicabilità**

1. La presente decisione è applicabile a decorrere dalla data determinata dalla Commissione ai sensi dell'articolo 48, paragrafo 1, del regolamento (CE) n. 767/2008.

2. La presente decisione scade quando l'Autorità di gestione entra in funzione.

Fatto a Bruxelles, il 4 maggio 2010.

*Per la Commissione*

*Il presidente*

José Manuel BARROSO