COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 4.10.2005
COM(2005) 475 definitivo

2005/0202 (CNS)

Proposta di

DECISIONE QUADRO DEL CONSIGLIO

sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale

{SEC(2005) 1241}

(presentata dalla Commissione)

RELAZIONE

1) CONTESTO DELLA PROPOSTA

- **Motivazione e obiettivi della proposta**

Il 4 novembre 2004 il Consiglio europeo ha adottato il programma dell'Aia sul rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea[1]. In tale programma si invita la Commissione a presentare entro la fine del 2005 proposte relative all'attuazione del principio di disponibilità al fine di migliorare lo scambio transfrontaliero di informazioni in materia di applicazione della legge tra Stati membri. Il programma dell'Aia sottolinea che nelle proposte dovrebbero essere rigorosamente osservate alcune condizioni fondamentali per quanto riguarda la protezione dei dati.

Nel giugno 2005 il Consiglio e la Commissione hanno adottato il piano d'azione sull'attuazione del programma dell'Aia[2] sulla base della comunicazione della Commissione al Consiglio e al Parlamento europeo intitolata "Dieci priorità per i prossimi cinque anni. Partenariato per rinnovare l'Europa nel campo della libertà, sicurezza e giustizia"[3]. Conformemente al piano d'azione, la Commissione deve presentare nel 2005 *proposte relative ai seguenti punti 1) l'adozione del principio della disponibilità delle informazioni in materia di applicazione della legge e 2) adeguate garanzie per il trasferimento di dati a carattere personale ai fini della cooperazione giudiziaria e di polizia in materia penale.* Il 13 luglio 2005 il Consiglio "Giustizia e Affari Interni", nella dichiarazione relativa alla risposta dell'UE agli attentati compiuti a Londra[4], ha chiesto alla Commissione di presentare tale proposta entro l'ottobre 2005.

La presente decisione quadro garantirà la protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale tra Stati membri dell'Unione europea (TUE, titolo VI). La decisione è finalizzata a migliorare tale cooperazione, in particolare per quanto riguarda la prevenzione e la lotta contro il terrorismo, nel rigoroso rispetto delle condizioni fondamentali relative alla protezione dei dati. Essa mira a garantire il rispetto dei diritti fondamentali, con particolare attenzione al diritto alla privacy e alla protezione dei dati personali, in tutta l'Unione europea, soprattutto ai fini dell'attuazione del principio di disponibilità. Inoltre, essa garantisce che lo scambio delle informazioni pertinenti tra Stati membri non sia intralciato dai diversi livelli di protezione dei dati negli Stati membri.

- **Contesto generale**

A seguito dell'iniziativa dell'Italia[5], si è già discusso nel 1998 della protezione dei dati personali nell'ambito del terzo pilastro. All'epoca, il Consiglio Giustizia e Affari Interni aveva adottato il cosiddetto Piano d'azione di Vienna[6] che stabiliva che – in relazione ai problemi orizzontali nel contesto della cooperazione giudiziaria e di polizia – le possibilità di norme armonizzate sulla protezione dei dati dovessero essere esaminate entro due anni dall'entrata in vigore del trattato. Tuttavia, nel 2001 non è stato adottato un progetto di

---

1 OJ C 53 del 3.3.2005, p. 1
2 GU C 198 del 12.8.2005, pag. 1.
3 COM(2005)184 def., Bruxelles, 10.5.2005
4 Documento di lavoro del Consiglio 11158/1/01 REV 1 JAI 255
5 Documento di lavoro del Consiglio 8321/98 JAI 15
6 GU C 19 del 23.1.1999, pag. 1.

risoluzione sulle norme per la protezione dei dati personali negli strumenti che rientrano nel terzo pilastro dell'Unione europea[7]. Nel giugno 2003 la Presidenza greca ha proposto una serie di principi generali sulla protezione dei dati personali nell'ambito del terzo pilastro[8], ispirati alla direttiva sulla protezione dei dati 95/46/CE e alla Carta dei diritti fondamentali dell'Unione europea. Nel 2005 le autorità responsabili della protezione dei dati degli Stati membri dell'Unione europea e il garante europeo della protezione dei dati (in appresso: GEPD) si sono espressi caldamente in favore di un nuovo strumento giuridico per la protezione dei dati nell'ambito del terzo pilastro[9]. Il Parlamento europeo ha raccomandato di armonizzare le norme esistenti in materia di protezione dei dati personali nell'ambito del terzo pilastro inserendole in uno strumento unico che garantisca lo stesso livello di protezione dei dati previsto dal primo pilastro[10].

Conformemente al programma dell'Aia, l'introduzione del principio di disponibilità è subordinata alle condizioni fondamentali per la protezione dei dati. Naturalmente, il Consiglio europeo ha ammesso che le disposizioni sulla protezione dei dati attualmente vigenti a livello europeo non sarebbero sufficienti per l'attuazione del principio di disponibilità in quanto quest'ultimo potrebbe comprendere anche modalità come l'accesso reciproco o diretto (on line) alle banche dati nazionali o l'interoperatività di queste ultime.

Emergono preoccupazioni riguardo all'adeguatezza della protezione dei dati anche in un accordo di cooperazione firmato il 27 maggio 2005 a Prüm da sette Stati membri (Germania, Austria, Belgio, Paesi Bassi, Lussemburgo, Francia e Spagna), accordo che tali Stati propongono come modello per lo scambio di informazioni tra gli Stati membri dell'Unione in generale. L'accordo prevede, a determinate condizioni specifiche, l'accesso diretto automatico per le autorità di contrasto di un paese contraente ai dati personali detenuti da un altro paese contraente. Ma tale forma di cooperazione non si applicherà finché le disposizioni in materia di protezione dei dati dell'accordo non saranno state recepite nei diritti nazionali dei paesi contraenti.

- **Disposizioni vigenti nelle materie oggetto della proposta**

La Carta dei diritti fondamentali dell'Unione europea[11] riconosce esplicitamente il diritto alla privacy (articolo 7) e il diritto alla protezione dei dati personali (articolo 8). Tali dati devono essere trattati in modo corretto, per specifiche finalità e sulla base del consenso della persona interessata o su un'altra base legittima prevista dalla legge. Ognuno ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

La direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla

---

7 Documento di lavoro del Consiglio 6316/2/01 REV 2 JAI 13

8 Riunione n. 2514 del Consiglio Giustizia e Affari Interni, Lussemburgo 5-6 giugno 2003, documento del Consiglio 9845/03(Stampa 150), pag. 32.

9 Dichiarazione e documento programmatico sull'applicazione della legge e lo scambio di informazioni nell'UE, adottati dalla conferenza di primavera delle autorità europee per la protezione dei dati, Cracovia, 25-26 aprile 2005.

10 Punto 1 h) della raccomandazione del Parlamento europeo al Consiglio europeo concernente lo scambio di informazioni e la cooperazione in materia di reati terroristici (2005/2046(INI), adottata il 7 giugno 2005.

11 GU C 364 del 18.12.2000, pagg. 1, 10.

libera circolazione di tali dati[12] contiene norme fondamentali sulla legittimità del trattamento dei dati personali e sui diritti della persona cui tali dati si riferiscono. Essa prevede disposizioni concernenti i ricorsi giurisdizionali, la responsabilità e le sanzioni, il trasferimento dei dati personali a paesi terzi, i codici di condotta, le specifiche autorità di controllo e il gruppo di lavoro e infine le norme comunitarie d'esecuzione. Tuttavia, la direttiva non si applica alle attività che non rientrano nel campo di applicazione della Comunità come quelle previste dal titolo VI del trattato sull'Unione europea (TUE). Pertanto, gli Stati membri sono autorizzati a decidere essi stessi quali siano le norme più adeguate per il trattamento e la protezione dei dati. Nell'ambito del titolo VI del TUE la protezione dei dati personali è disciplinata da diversi strumenti specifici e, segnatamente, da strumenti che istituiscono sistemi comuni di informazioni a livello europeo come la convenzione di applicazione dell'accordo di Schengen del 1990 che comprende disposizioni specifiche sulla protezione dei dati applicabili al sistema d'informazione Schengen[13]; la convenzione Europol del 1995[14] e, tra l'altro, le norme che disciplinano la trasmissione dei dati personali da Europol a Stati e organismi terzi[15]; la decisione del 2002 che istituisce Eurojust[16] e le norme procedurali sul trattamento e la protezione dei dati personali di Eurojust[17]; la convenzione sull'uso dell'informatica nel settore doganale del 1995 che comprende disposizioni sulla protezione dei dati personali applicabili al Sistema di informazioni delle dogane[18]; la convenzione sull'assistenza reciproca in materia penale tra gli Stati membri dell'Unione europea del 2000 e segnatamente l'articolo 23[19]. Per quanto riguarda il sistema d'informazione Schengen, occorre tener particolarmente conto della creazione, messa in opera e utilizzazione del sistema d'informazione Schengen di seconda generazione (SIS II) per il quale la Commissione ha già presentato una proposta di decisione del Consiglio[20] e due regolamenti[21].

Inoltre, occorre tener conto dell'articolo 8 della convenzione sulla protezione dei diritti umani e delle libertà fondamentali e della convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del 1981, del suo protocollo aggiuntivo del 2001 relativo alle autorità di controllo e i flussi transfrontalieri, e della raccomandazione n. R (87) 15 del 1987 che disciplina l'uso dei dati personali nel settore della polizia. Tutti gli Stati membri partecipano alla convenzione ma non tutti hanno firmato il protocollo aggiuntivo.

- **Coerenza con altri obiettivi e politiche dell'Unione**

È necessario rendersi conto della peculiarità del trattamento e della protezione dei dati nel quadro del titolo VI del trattato sull'Unione europea. Da una parte, infatti, essi non devono ostacolare la coerenza con la politica generale dell'Unione nel settore della privacy e della protezione dei dati sulla base della Carta per i diritti fondamentali dell'UE e della direttiva 95/46/CE. I principi fondamentali della protezione dei dati si applicano al

---

12 GU C 281 del 23.11.1995, pag. 31.
13 GU C 239 del 22.09.2000, pag. 19.
14 GU C 316 del 27.11.1995, pag. 2.
15 GU C 88 del 30.3.1999, pag. 1.
16 GU C 63 del 6.3.2002, pag. 1.
17 GU C 68 del 19.3.2005, pag. 1.
18 GU C 316 del 27.11.1995, pag. 34.
19 GU C 197 del 12.7.2000, pagg. 1, 15.
20 COM(2005) 230 def.
21 COM (2005) 236 def., COM (2005) 237 def.

trattamento dei dati nell'ambito del primo e del terzo pilastro. D'altra parte, deve essere garantita la coerenza con altri strumenti che prevedono obblighi specifici in relazione alle informazioni che potrebbero essere rilevanti ai fini della prevenzione e della lotta contro la criminalità. Occorre tener conto degli sviluppi concernenti la conservazione e la memorizzazione dei dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica o dei dati delle reti di comunicazioni pubbliche al fine della prevenzione, delle indagini e del perseguimento della criminalità e dei reati penali tra cui il terrorismo. In particolare, bisogna tener conto della stretta relazione tra la proposta di decisione quadro e la proposta della Commissione di una direttiva del Parlamento europeo e del Consiglio riguardante la memorizzazione dei dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica che modifica la direttiva 2002/58/CE.[22]

2) CONSULTAZIONE DELLE PARTI INTERESSATE E VALUTAZIONE DELL'IMPATTO

- **Consultazione**

Metodi di consultazione, principali settori consultati e profilo generale di quanti hanno risposto

Il 22 novembre 2004 e il 21 giugno 2005 la Commissione ha invitato e consultato gli esperti dei governi degli Stati membri, dell'Islanda, della Norvegia e della Svizzera e l'11 gennaio 2005 gli esperti delle autorità responsabili della protezione dei dati di tali Stati. Erano rappresentati anche il GEPD, Europol, Eurojust e il Segretariato delle autorità di controllo comuni. Lo scopo principale delle consultazioni era di valutare la necessità di uno strumento giuridico per il trattamento e la protezione dei dati personali per quanto riguarda il terzo pilastro ed, eventualmente, di individuare quale dovesse essere il contenuto principale di tale strumento. La Commissione, sulla base di un questionario e di un documento di riflessione, ha chiesto, tra l'altro, alle parti interessate la loro posizione per quanto riguarda l'approccio generale da adottare per la creazione di un nuovo strumento giuridico e i suoi collegamenti con gli strumenti esistenti, la base giuridica, l'eventuale campo di applicazione, i principi relativi alla qualità dei dati, i criteri per rendere legittimo il trattamento dei dati da parte delle autorità giudiziarie e di polizia, i dati personali delle persone non sospette, le condizioni da soddisfare per la trasmissione dei dati personali alle autorità competenti in altri Stati membri e in paesi terzi, i diritti degli interessati, le autorità di controllo e un eventuale organo consultivo per la protezione dei dati nell'ambito del terzo pilastro.

Il gruppo di lavoro, costituito conformemente all'articolo 29 della direttiva 95/46/CE, è stato regolarmente informato sugli sviluppi in corso. Il 12 aprile e il 21 giugno 2005 la Commissione ha partecipato alle riunioni del gruppo di lavoro della polizia nell'ambito della conferenza delle autorità europee responsabili della protezione dei dati. Il 31 gennaio 2005 la Commissione ha partecipato a un "Seminario pubblico: protezione dei dati e sicurezza dei cittadini: quali principi per l'Unione europea?" organizzato dalla commissione per le libertà civili, la giustizia e gli affari interni del Parlamento. La Commissione ha tenuto conto dei risultati della conferenza di aprile delle autorità europee responsabili della protezione dei dati (Cracovia, 25-26 aprile 2005) e della posizione del Parlamento europeo esposta, tra l'altro, nella raccomandazione del Parlamento europeo e del Consiglio sullo scambio di informazioni e la cooperazione in materia di reati terroristici (2005/2046(INI), adottata il 7 giugno 2005.

---

[22] COM(2005) 438 def. del 21.9.2005.

Sintesi delle risposte e modo in cui sono state prese in considerazione

Sia il Parlamento europeo che le autorità responsabili della protezione dei dati nell'Unione europea sono estremamente favorevoli a uno strumento giuridico sulla protezione dei dati personali nell'ambito del terzo pilastro. I rappresentanti dei Governi degli Stati membri, dell'Islanda, della Norvegia e della Svizzera e di Europol e Eurojust non hanno espresso una posizione comune in materia. La Commissione, tuttavia, ha potuto concludere che non c'era un'opposizione di principio all'idea di un tale strumento. Sembra esservi un accordo sul fatto che l'attuazione del principio di disponibilità deve essere accompagnata da adeguate norme di compensazione nel settore della protezione dei dati. Alcuni Stati membri hanno dichiarato che occorre prima definire le modalità dello scambio futuro di informazioni e successivamente le norme per la protezione dei dati. Alcuni Stati erano invece più a favore dell'inserimento di una serie di disposizioni specifiche nell'atto relativo al principio di disponibilità.

Dopo aver valutato le diverse posizioni, la Commissione ha deciso che l'attuazione del principio di disponibilità, che cambierà sostanzialmente la qualità e l'intensità dello scambio di informazioni tra Stati membri, deve essere portata avanti. Si tratta di uno sviluppo che avrà conseguenze rilevanti per i dati personali e il diritto alla protezione dei dati e che deve essere opportunamente compensato. Iniziative recenti finalizzate all'accesso diretto automatico, almeno sulla base del sistema hit/no hit aumenteranno probabilmente il rischio di scambio di dati illegali, non accurati o non aggiornati e di ciò occorre tener conto. Tali iniziative portano a far sì che il responsabile del controllo non sia in grado di verificare *in ciascun caso* la legittimità di una trasmissione e l'accuratezza dei dati in questione. Pertanto, devono esservi obblighi severi di garantire e di verificare costantemente la qualità dei dati a cui viene dato l'accesso diretto automatico.

Le disposizioni relative a singoli aspetti della protezione dei dati e incentrate sull'impatto dell'attuazione del principio di disponibilità non sono sufficienti. Uno strumento giuridico relativo alla protezione dei dati personali nell'ambito del terzo pilastro può, in linea di principio, contribuire a instaurare una cooperazione giudiziaria e di polizia in materia penale per quanto riguarda l'efficacia e la legittimità e conformità con i diritti fondamentali, e, segnatamente, il diritto alla protezione dei dati personali.

In particolare, ai fini dell'attuazione del principio di disponibilità, uno strumento di questo tipo è particolarmente necessario e deve essere elaborato di pari passo con l'attuazione di tale principio. La decisione quadro deve rifarsi, per quanto possibile, allo spirito e alla struttura della direttiva 95/46/CE, pur tenendo conto delle esigenze specifiche della cooperazione giudiziaria e di polizia in materia penale e nell'ottica del principio di proporzionalità. Si è tenuto conto della raccomandazione n. R(87)15 che disciplina l'utilizzazione dei dati personali nel settore di polizia del Consiglio d'Europa del 1987 al fine di recepirne i principi essenziali in disposizioni giuridicamente vincolanti a livello dell'UE. Devono essere istituite norme chiare per la protezione dei dati personali che saranno o sono stati resi disponibili alle autorità competenti degli altri Stati membri. Ciò richiede un sistema che garantisca la qualità del trattamento di tali dati. Tale sistema deve comprendere disposizioni che stabiliscano i diritti di coloro cui i dati si riferiscono e i poteri delle autorità di controllo dal momento che l'esercizio di tali diritti e poteri può contribuire alla qualità dei dati in questione.

- **Valutazione dell'impatto**

Sono state esaminate le seguenti possibilità: applicabilità della direttiva 95/46/CE; nessuna proposta o una proposta successiva per la protezione dei dati personali nell'ambito del terzo

pilastro; una serie limitata di disposizioni specifiche in un atto giuridico in relazione allo scambio di informazioni nell'ambito della protezione dei dati personali; una decisione quadro sulla protezione dei dati personali nell'ambito del terzo pilastro. Per quanto riguarda quest'ultima si è valutato se tale strumento dovesse applicarsi anche allo scambio di informazioni tra sistemi e organi di informazione istituiti a livello dell'UE.

Le disposizioni generali fondamentali della direttiva 95/46/CE non sono applicabili nell'ambito del terzo pilastro, come specifica l'articolo 3, paragrafo 2. Neanche la soppressione di questo articolo porterebbe automaticamente all'applicabilità della direttiva alla cooperazione giudiziaria e di polizia in materia penale. Prima di tutto, poiché la direttiva non esamina fino in fondo le peculiarità di tale cooperazione, sarebbero necessarie ulteriori precisazioni. In secondo luogo, devono essere rispettate le esigenze relative alla legislazione adottata nell'ambito del titolo VI del trattato sull'Unione europea che si propone di consolidare la cooperazione giudiziaria e di polizia in materia penale. L'opzione "nessuna proposta o una proposta successiva per la protezione dei dati personali nell'ambito del terzo pilastro" deve essere esclusa. Tale opzione potrebbe portare, con l'attuazione del principio di disponibilità, all'introduzione di nuove forme di scambi di informazioni senza la garanzia del rispetto delle condizioni fondamentali per quanto riguarda la protezione dei dati. Una serie limitata di disposizioni specifiche in un atto giuridico concernente lo scambio di informazioni nell'ambito del principio di disponibilità non è sufficiente, considerato il probabile impatto di quest'ultimo. Una decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale è l'unica opzione soddisfacente. È un'opzione che difficilmente comporterà costi amministrativi rilevanti – se mai ci saranno dei costi – per gli Stati membri.

La Commissione ha effettuato una valutazione d'impatto che viene presentata nel programma di lavoro mentre la relazione sulla valutazione d'impatto è consultabile al seguente indirizzo Internet:
http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3) ELEMENTI GIURIDICI DELLA PROPOSTA

- **Sintesi delle misure proposte**

La proposta di decisione quadro comprende norme generali sulla legittimità del trattamento dei dati personali e disposizioni concernenti: le forme specifiche di trattamento (trasmissione e messa a disposizione di dati personali alle autorità competenti degli altri Stati membri, ulteriore trattamento, segnatamente ulteriore trasmissione, dei dati ricevuti o resi disponibili dalle autorità competenti degli altri Stati membri); i diritti delle persone cui i dati si riferiscono; la riservatezza e la sicurezza del trattamento; i ricorsi giurisdizionali; le responsabilità; le sanzioni; le autorità di controllo e un gruppo di lavoro sulla protezione delle persone con riguardo al trattamento dei dati personali ai fini della prevenzione, della ricerca, dell'accertamento e del perseguimento dei reati penali. Occorre, in particolare, che si tenga conto del principio secondo cui i dati a carattere personale devono essere trasmessi solo ai paesi terzi e agli organi internazionali che garantiscono un livello adeguato di protezione. La decisione quadro prevede un meccanismo finalizzato ad assicurare il rispetto di tale principio in tutta l'UE.

- **Base giuridica**

La presente decisione quadro si basa sugli articoli 30, 31 e 34, paragrafo 2, lettera b) del trattato sull'Unione europea. Soprattutto in considerazione dell'attuazione del principio di disponibilità sono indispensabili disposizioni adeguate sul trattamento e la protezione dei dati personali, comprese norme comuni per la trasmissione di tali dati a paesi terzi e organi internazionali, per migliorare la cooperazione giudiziaria e di polizia in materia penale, segnatamente ai fini della lotta contro il terrorismo e i reati gravi. Inoltre, gli Stati membri avranno piena fiducia reciproca soltanto se vi saranno norme comuni chiare sull'eventuale ulteriore trasmissione dei dati scambiati ad altri ed in particolare a paesi terzi. Le disposizioni proposte garantiranno che lo scambio di informazioni tra le autorità competenti non venga pregiudicato da livelli diversi di protezione dei dati negli Stati membri.

- **Principi di sussidiarietà e di proporzionalità**

La presente decisione quadro riguarda situazioni di particolare rilevanza per la cooperazione giudiziaria e di polizia in materia penale tra gli Stati membri, soprattutto in relazione allo scambio di informazioni al fine di garantire e promuovere misure efficaci e lecite per prevenire e combattere la criminalità ed in particolare i reati gravi e il terrorismo in *tutti* gli Stati membri. Soluzioni nazionali, bilaterali o multilaterali potrebbero essere utili per i singoli Stati membri ma non terrebbero conto della necessità di garantire la sicurezza interna in tutta l'Unione. La necessità di informazioni avvertita dalle autorità di contrasto è determinata in gran parte dal livello di integrazione tra paesi. Si ritiene che lo scambio di informazioni tra Stati membri ai fini delle attività di contrasto sia destinato a crescere e debba pertanto essere accompagnato da norme coerenti in materia di trattamento e protezione dei dati. La presente decisione quadro rispetta il principio di sussidiarietà previsto dall'articolo 2 del trattato sull'Unione europea e dall'articolo 5 del trattato che istituisce la Comunità europea dal momento che intende ravvicinare le leggi e i regolamenti degli Stati membri, cosa che non può essere fatta in maniera adeguata se gli Stati membri agiscono unilateralmente ma richiede un'azione concertata a livello dell'Unione europea. Nel rispetto del principio di proporzionalità, enunciato nel medesimo articolo, la presente decisione non va al di là di quanto è necessario per conseguire il suddetto obiettivo. In particolare, la presente decisione si riferisce soltanto al trattamento dei dati personali ai fini della cooperazione giudiziaria e di polizia in materia penale.

- **Scelta dello strumento**

Lo strumento proposto è una decisione quadro. Tale strumento giuridico intende ravvicinare le leggi e i regolamenti degli Stati membri relativi alla protezione dei dati personali trattati ai fini della prevenzione e della lotta contro la criminalità.

4) INCIDENZA SUL BILANCIO

L'attuazione della presente proposta di decisione quadro comporterebbe spese amministrative supplementari solo di lieve entità, da addebitare al bilancio delle Comunità europee, per le riunioni e i servizi di segreteria per il comitato e l'organo consultivo da istituire conformemente all'articolo 16 e all'articolo 31.

2005/0202 (CNS)

Proposta di

DECISIONE QUADRO DEL CONSIGLIO

sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sull'Unione europea, in particolare l'articolo 30, l'articolo 31 e l'articolo 34, paragrafo 2, lettera b),

vista la proposta della Commissione[23],

visto il parere del Parlamento europeo[24],

considerando quanto segue:

(1) L'Unione europea si è posta l'obiettivo di far sì che l'Unione sia e si sviluppi come uno spazio di libertà, sicurezza e giustizia; un elevato livello di sicurezza è offerto dalle azioni comuni degli Stati membri nel settore della cooperazione giudiziaria e di polizia in materia penale.

(2) Le azioni comuni nel settore della cooperazione di polizia ai sensi dell'articolo 30, paragrafo 1, lettera b) del trattato sull'Unione europea e le azioni comuni nel settore della cooperazione giudiziaria in materia penale ai sensi dell'articolo 31, paragrafo 1, lettera a) del trattato sull'Unione europea richiedono un trattamento delle informazioni rilevanti che deve essere disciplinato da adeguate disposizioni sulla protezione dei dati personali.

(3) La legislazione che rientra nell'ambito del titolo VI del trattato sull'Unione europea dovrebbe rafforzare la cooperazione giudiziaria e di polizia in materia penale per quanto riguarda l'efficacia e la legittimità e il rispetto dei diritti fondamentali, soprattutto il diritto alla privacy e alla protezione dei dati personali. Le norme comuni sul trattamento e la protezione dei dati personali trattati ai fini della prevenzione e della lotta contro la criminalità possono contribuire a raggiungere entrambi gli obiettivi.

(4) Il programma dell'Aia sul rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea adottato dal Consiglio europeo il 4 novembre 2004 ha sottolineato la necessità di un approccio innovativo allo scambio transfrontaliero di informazioni in materia di applicazione della legge nel rigoroso rispetto delle condizioni fondamentali

---

23 …

24 …

per quanto riguarda la protezione dei dati e ha invitato la Commissione a presentare proposte in proposito entro la fine del 2005. Ciò ha trovato riscontro nel piano d'azione del Consiglio e della Commissione per l'attuazione del programma dell'Aia sul rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea[25].

(5) Lo scambio dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale, segnatamente in conformità del principio di disponibilità delle informazioni stabilito dal programma dell'Aia, deve essere disciplinato da norme vincolanti chiare che rafforzino la fiducia reciproca delle autorità competenti e garantiscano che le informazioni rilevanti siano protette in modo da escludere qualsiasi intralcio alla cooperazione tra Stati membri pur nel pieno rispetto dei diritti fondamentali dell'individuo. Gli strumenti esistenti a livello europeo non sono sufficienti. La direttiva 95/46 del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[26] non si applica al trattamento dei dati personali nel corso di attività che esulino dal campo di applicazione della normativa comunitaria, come quelle previste dal titolo VI del trattato sull'Unione europea e, in ogni caso, ai trattamenti dati relativi alla sicurezza pubblica, alla difesa, alla sicurezza di Stato e alle attività dello Stato in materia di diritto penale.

(6) Uno strumento giuridico relativo a norme comuni per la protezione dei dati personali trattati ai fini della prevenzione e della lotta contro la criminalità deve essere coerente con la politica generale dell'Unione europea in materia di privacy e protezione dei dati. Esso dovrebbe, pertanto, rifarsi, per quanto possibile e tenendo conto della necessità di migliorare l'efficacia delle attività legittime delle autorità giudiziarie, doganali, di polizia e delle altre autorità competenti, ai principi e definizioni esistenti e già dimostrati, segnatamente quelli contenuti nella direttiva 95/46/CE del Parlamento europeo e del Consiglio o quelli che riguardano lo scambio di informazioni di Europol e Eurojust o trattati mediante il sistema di informazione doganale o altri strumenti affini.

(7) Il ravvicinamento delle leggi degli Stati membri non deve portare ad una riduzione del livello di protezione dei dati ma deve, al contrario, cercare di garantire che esso sia elevato in tutta l'Unione.

(8) È necessario specificare quali sono gli obiettivi della protezione dei dati nell'ambito delle attività giudiziarie e di polizia e istituire norme sulla legittimità del trattamento dei dati personali al fine di garantire che tutte le informazioni che possono essere scambiate siano state trattate in maniera legittima e conformemente ai principi fondamentali in materia di qualità dei dati. Al tempo stesso, le legittime attività delle autorità giudiziarie, doganali, di polizia e delle altre autorità competenti non devono in alcun modo essere compromesse.

(9) Per garantire un elevato livello di protezione dei dati personali dei cittadini europei sono necessarie disposizioni comuni per determinare la legittimità e la qualità dei dati trattati dalle autorità competenti in altri Stati membri.

---

[25] GU C 198 del 12.08.2005, pag. 1.
[26] GU C 281 del 23.11.1995, pag. 31.

(10) È opportuno fissare a livello europeo le condizioni alle quali le autorità competenti degli Stati membri possono essere autorizzate a trasmettere e rendere disponibili i dati personali alle autorità e ai privati in altri Stati membri.

(11) L'ulteriore trattamento dei dati personali ricevuti o resi disponibili dalle autorità competenti di un altro Stato membro e, in particolare, l'ulteriore trasmissione o messa a disposizione di tali dati devono essere disciplinati da norme comuni a livello europeo.

(12) Qualora i dati personali siano trasferiti da uno Stato membro dell'Unione europea a paesi terzi o organismi internazionali, tali dati devono, in linea di principio, godere di un adeguato livello di protezione.

(13) La presente decisione quadro definisce il procedimento per l'adozione delle misure necessarie per valutare il livello della protezione dei dati in un paese terzo o organismo internazionale.

(14) Al fine di garantire la protezione dei dati personali senza compromettere le indagini penali è necessario definire i diritti di coloro cui i dati si riferiscono.

(15) È opportuno stabilire norme comuni sulla riservatezza e la sicurezza del trattamento, sulla responsabilità e le sanzioni in caso di uso illegittimo da parte delle autorità competenti e sui ricorsi giurisdizionali che coloro cui si riferiscono i dati possono utilizzare. Inoltre, è necessario che gli Stati membri prevedano sanzioni penali per le violazioni particolarmente gravi e intenzionali delle disposizioni per la protezione dei dati.

(16) L'istituzione negli Stati membri di autorità di controllo, che esercitino le proprie funzioni in piena indipendenza, è una componente essenziale della protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

(17) Tali autorità devono disporre dei mezzi necessari all'adempimento dei loro compiti, siano essi poteri investigativi o di intervento, segnatamente in caso di reclami di singoli individui, nonché poteri di avviare azioni legali. Tali autorità devono contribuire alla trasparenza dei trattamenti effettuati nello Stato membro da cui dipendono. Tuttavia, i poteri di tali autorità non devono interferire con le norme specifiche stabilite per i procedimenti penali e con l'indipendenza della magistratura.

(18) Deve essere costituito un gruppo di lavoro per la tutela delle persone fisiche con riguardo al trattamento dei dati personali al fine della prevenzione, delle indagini e del perseguimento dei reati penali. Tale gruppo deve essere completamente indipendente nell'esercizio delle proprie funzioni. Il gruppo deve fornire consulenza alla Commissione e agli Stati membri e, segnatamente, contribuire all'applicazione uniforme delle norme nazionali adottate conformemente alla presente decisione quadro.

(19) L'articolo 47 del trattato sull'Unione europea prevede che nessuna sua disposizione pregiudichi i trattati che istituiscono le Comunità europee né i trattati e atti successivi che li hanno modificati o completati. Conformemente a ciò, la decisione quadro non pregiudica la protezione dei dati personali ai sensi del diritto comunitario,

segnatamente, ai sensi di quanto previsto dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, dal regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati[27] e dalla direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)[28].

(20) La presente decisione quadro non pregiudica le disposizioni specifiche per la protezione dei dati previste dagli strumenti giuridici in materia di trattamento e protezione dei dati personali di Europol, Eurojust e del sistema di informazione doganale.

(21) Le disposizioni relative alla protezione dei dati personali, previste dal titolo IV della convenzione di applicazione dell'accordo di Schengen relativo all'eliminazione graduale dei controlli alle frontiere comuni[29] del 1990 (in appresso "convenzione di Schengen") e integrate nell'ambito dell'Unione europea in virtù del protocollo allegato al trattato sull'Unione europea e al trattato che istituisce la Comunità europea, sono sostituite dalle norme della presente decisione quadro per quanto rientra nell'ambito di applicazione del trattato UE.

(22) È opportuno che la presente decisione quadro si applichi ai dati personali trattati nell'ambito della seconda generazione del sistema di informazione Schengen e al relativo scambio di informazioni supplementari ai sensi della decisione GAI/2006/… sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione.

(23) La presente decisione quadro non pregiudica le norme relative all'accesso illecito ai dati previste dalla decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione[30].

(24) È opportuno sostituire l'articolo 23 della convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea[31].

(25) Qualsiasi riferimento alla convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale del 28 gennaio 1981 deve essere considerato come un riferimento alla presente decisione quadro.

(26) Poiché gli obiettivi dell'azione proposta, ossia definire norme comuni per la protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, non possono essere conseguiti in misura sufficiente dagli Stati membri, ma possono, a motivo delle dimensioni e degli effetti dell'azione, essere realizzati meglio a livello dell'Unione europea, il Consiglio può adottare

---

27 GU C 8 del 12.01.2001, pag. 1.
28 GU C 201 del 31.07.2002, pag. 37.
29 GU C 239 del 22.09.2000, pag. 19.
30 GU C 69 del 13.03.2005, pag. 67.
31 GU C 197 del 12.07.2000, pag. 3.

provvedimenti ai sensi del principio di sussidiarietà definito all'articolo 5 del trattato CE e richiamato all'articolo 2 del trattato UE. Conformemente al principio di proporzionalità enunciato all'articolo 5 del trattato CE, la presente decisione quadro non va al di là di quanto necessario per il raggiungimento dei suddetti obiettivi.

(27) Il Regno Unito partecipa alla presente decisione, ai sensi dell'articolo 5 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea allegato al trattato sull'Unione europea e al trattato che istituisce la Comunità europea, e dell'articolo 8, paragrafo 2, della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen[32].

(28) L'Irlanda partecipa alla presente decisione, ai sensi dell'articolo 5 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea allegato al trattato sull'Unione europea e al trattato che istituisce la Comunità europea, e dell'articolo 6, paragrafo 2, della decisione 2002/192/CE del Consiglio, del 28.2.02, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen.

(29) In relazione all'Islanda e alla Norvegia, la presente decisione quadro costituisce uno sviluppo dell'acquis di Schengen ai sensi dell'accordo concluso tra il Consiglio dell'Unione europea e la Repubblica d'Islanda e il Regno di Norvegia sull'associazione di questi due Stati all'attuazione, applicazione e sviluppo dell'acquis di Schengen, che rientra nel settore contemplato all'articolo 1, lettera H, della decisione 1999/437/CE del Consiglio, del 17 maggio 1999, relativa ad alcune modalità per l'applicazione del suddetto accordo[33].

(30) In relazione alla Svizzera, la presente decisione quadro costituisce uno sviluppo dell'acquis di Schengen ai sensi dell'accordo firmato dall'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, applicazione e sviluppo dell'acquis di Schengen, che ricade nell'ambito contemplato all'articolo 1, lettera H, della decisione 1999/437/CE, in combinato disposto con l'articolo 4, paragrafo 1, della decisione 2004/849/CE del Consiglio relativa alla firma, a nome della Comunità europea, nonché all'applicazione provvisoria di alcune disposizioni del suddetto accordo[34].

(31) La presente decisione quadro costituisce un atto fondato sull'acquis di Schengen o altrimenti ad esso correlato ai sensi dell'articolo 3, paragrafo 1, dell'atto di adesione del 2003.

(32) La presente decisione quadro rispetta i diritti fondamentali e osserva i principi sanciti in particolare dalla Carta dei diritti fondamentali dell'Unione europea. La presente decisione quadro cerca di garantire il pieno rispetto dei diritti alla privacy e alla protezione dei dati personali di cui agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

---

32 GU C 131 del 01.06.2000, pag. 43.
33 GU C 176 del 10.07.1999, pag. 31.
34 GU C 368 del 15.12.2004, pag. 26.

HA ADOTTATO LA PRESENTE DECISIONE QUADRO:

CAPITOLO I

Obiettivi, definizioni e portata

Articolo 1
Oggetto

1. La presente decisione quadro definisce norme comuni per garantire la protezione delle persone riguardo al trattamento dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale di cui al titolo VI del trattato sull'Unione europea.

2. Gli Stati membri garantiscono che la divulgazione dei dati personali alle autorità competenti degli altri Stati membri non sia limitata né proibita per motivi legati alla protezione dei dati personali di cui alla presente decisione quadro.

Articolo 2
Definizioni

Ai fini della presente decisione quadro s'intende per:

(a) «dati personali»: qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;

(b) «trattamento di dati personali» («trattamento»): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione;

(c) «archivio di dati personali» («archivio»): qualsiasi insieme strutturato di dati personali accessibili, secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

(d) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Qualora le finalità e gli strumenti del trattamento siano definiti dal diritto nazionale o dalla legislazione adottata conformemente al titolo VI del trattato sull'Unione europea, il responsabile può essere designato o i criteri specifici per la sua nomina possono essere stabiliti dal

diritto nazionale o dalla legislazione adottata conformemente al titolo VI del trattato sull'Unione europea;

(e) «incaricato del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento;

(f) «terzi»: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia la persona interessata, il responsabile del trattamento, l'incaricato del trattamento e le persone autorizzate all'elaborazione dei dati sotto la loro autorità diretta;

(g) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che riceve comunicazione di dati, che si tratti o meno di un terzo;

(h) «consenso della persona interessata»: qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento;

(i) "organismi internazionali": organismi o organizzazioni istituiti sulla base di accordi internazionali;

(j) "autorità competenti": autorità giudiziarie, doganali, di polizia e altre autorità competenti degli Stati membri ai sensi dell'articolo 29 del trattato sull'Unione europea.

Articolo 3
Campo d'applicazione

1. La presente decisione quadro si applica al trattamento di dati personali, interamente o parzialmente automatizzato, nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi da parte di un'autorità competente ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati penali.

2. Le disposizioni della presente decisione quadro non si applicano ai trattamenti dei dati personali effettuati:

   – dall'Ufficio europeo di polizia (Europol),

   – dall'Unità europea di cooperazione giudiziaria (Eurojust),

   – dal sistema di informazione delle dogane costituito conformemente alla convenzione stilata sulla base dell'articolo K.3 del trattato sull'Unione europea sull'uso della tecnologia informatica ai fini doganali e successive modifiche.

CAPITOLO II
CONDIZIONI GENERALI DI LEGITTIMITÀ DEL TRATTAMENTO DI DATI PERSONALI

Articolo 4
Principi relativi alla qualità dei dati

1. Gli Stati membri dispongono che i dati personali devono essere:

   (a) trattati correttamente e lecitamente;

   (b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;

   (c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;

   (d) esatti e, se necessario, aggiornati. Devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono raccolti o successivamente trattati. Gli Stati membri possono disporre per il trattamento dei dati diversi livelli di accuratezza ed affidabilità; in tal caso, devono provvedere a distinguere i dati sulla base del loro livello di accuratezza ed affidabilità e, segnatamente, a distinguere i dati basati sui fatti dai dati basati su opinioni e considerazioni personali;

   (e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.

2. Il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1.

3. Gli Stati membri provvedono ad effettuare una chiara distinzione tra i dati personali relativi a

   – una persona sospettata di aver commesso o di essere stata complice di un reato penale,

   – una persona condannata per un reato penale,

   – una persona che dia adito a ritenere che commetterà un reato penale,

   – una persona che potrebbe essere convocata per testimoniare in indagini relative a reati penali o ai successivi procedimenti penali,

   – una persona che sia stata vittima di un reato penale o che dia ragionevolmente adito a ritenere che possa essere vittima di un reato penale,

   – una persona che possa fornire informazioni su reati penali,

– una persona che è in contatto o è collegata alle persone di cui sopra,

– una persona che non rientra nelle categorie di cui sopra.

4. Gli Stati membri dispongono affinché tale trattamento dei dati sia necessario soltanto se

– vi sono ragionevoli motivi, sulla base di fatti accertati, per credere che i dati personali in questione rendano possibili, agevolino o accelerino la prevenzione, le indagini, l'accertamento o il perseguimento di un reato penale,

– non vi siano altri mezzi meno invasivi per la persona cui i dati si riferiscono,

– il trattamento dei dati non sia eccessivo rispetto al reato in questione.

Articolo 5
Principi relativi alla legittimazione del trattamento dei dati.

Gli Stati membri dispongono affinché i dati personali siano trattati dalle autorità competenti soltanto se ciò è previsto da una legge che stabilisca che il trattamento dei dati è necessario per svolgere i compiti legittimi dell'autorità interessata e ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali.

Articolo 6
Trattamenti riguardanti categorie particolari di dati

1. Gli Stati membri vietano il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale.

2. Il paragrafo 1 non si applica qualora:

– il trattamento sia previsto da una legge e sia assolutamente necessario per l'adempimento delle legittime funzioni dell'autorità interessata ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali o se la persona cui i dati si riferiscono ha dato il proprio esplicito consenso al trattamento

– gli Stati membri prevedono specifici ed adeguati meccanismi di salvaguardia, per esempio che l'accesso ai dati interessati sia permesso solo al personale responsabile dell'adempimento dei compiti legittimi che giustificano tale trattamento.

Articolo 7
Limiti di tempo per la memorizzazione dei dati personali

1. Gli Stati membri dispongono affinché i dati personali non siano memorizzati per un tempo più lungo di quanto necessario per lo scopo per il quale siano stati raccolti, tranne che nei casi in cui il diritto nazionale stabilisca diversamente. I dati personali

relativi alle persone di cui all'articolo 4, paragrafo 3, ultimo trattino, sono memorizzati solo per il tempo assolutamente necessario allo scopo per il quale sono stati raccolti.

2. Gli Stati membri prevedono adeguate misure procedurali e tecniche per garantire che i limiti di tempo per la memorizzazione dei dati personali siano rispettati. Il rispetto di tali limiti di tempo è regolarmente verificato.

CAPITOLO III – Forme specifiche di trattamento

SEZIONE I – TRASMISSIONE E MESSA A DISPOSIZIONE DI DATI PERSONALI ALLE AUTORITÀ COMPETENTI DI ALTRI STATI MEMBRI

Articolo 8
Trasmissione e messa a disposizione di dati personali alle autorità competenti di altri Stati membri

Gli Stati membri dispongono affinché i dati personali siano trasmessi o resi disponibili alle autorità competenti degli altri Stati membri soltanto se necessario per l'adempimento di un compito legittimo dell'autorità che trasmette o che riceve e ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali.

Articolo 9
Verifica della qualità dei dati trasmessi o resi disponibili

1. Gli Stati membri dispongono affinché la qualità dei dati personali sia verificata prima che questi siano trasmessi o resi disponibili. Nei limiti del possibile, in tutte le trasmissioni di dati, devono essere indicate le decisioni giudiziarie e le decisioni di proscioglimento e i dati basati su opinioni o considerazioni personali devono essere verificati alla fonte prima di essere trasmessi e occorre indicare il loro livello di accuratezza e affidabilità.

2. Gli Stati membri dispongono affinché la qualità dei dati personali, resi disponibili mediante l'accesso diretto automatico alle autorità competenti degli altri Stati membri, sia regolarmente verificata al fine di garantire che i dati cui si dà l'accesso siano precisi ed aggiornati.

3. Gli Stati membri dispongono affinché i dati personali che non sono più precisi o aggiornati non siano trasmessi o resi disponibili.

4. Gli Stati membri dispongono affinché l'autorità competente che ha trasmesso o reso disponibili i dati personali a un'autorità competente di un altro Stato membro informi immediatamente quest'ultimo qualora accerti, di propria iniziativa o in seguito a una richiesta della persona cui si riferiscono i dati, che tali dati non dovevano essere trasmessi o resi disponibili o che sono stati trasmessi o resi disponibili dati imprecisi o non aggiornati.

5. Gli Stati membri dispongono affinché l'autorità competente informata conformemente al paragrafo 4 cancelli o rettifichi i dati in questione. Inoltre, tale autorità, qualora dovesse accertare che i dati in questione sono imprecisi, è tenuta a rettificarli. Qualora abbia ragionevoli motivi per credere che i dati personali ricevuti siano imprecisi o debbano essere cancellati, tale autorità è tenuta ad informare immediatamente l'autorità competente che ha trasmesso o reso disponibili i dati in questione.

6. Gli Stati membri dispongono che, fatta salva la procedura penale nazionale, i dati personali siano contrassegnati su richiesta della persona interessata qualora questa ritenga che essi non siano precisi e qualora non possa essere accertato se essi siano o meno precisi. Tale contrassegno viene cancellato solo previo consenso dell'interessato o sulla base di una decisione del tribunale competente o dell'autorità di controllo competente.

7. Gli Stati membri dispongono affinché i dati personali ricevuti dall'autorità di un altro Stato membro siano cancellati nei seguenti casi:

   – se tali dati non avrebbero dovuto essere trasmessi, resi disponibili o ricevuti,

   – dopo un termine stabilito dalla legislazione dell'altro Stato membro se l'autorità che ha trasmesso o reso disponibili i dati in questione ha informato l'autorità ricevente di tale termine quando sono stati trasmessi o resi disponibili tali dati, a meno che i dati personali non servano ulteriormente per un procedimento giudiziario,

   – se tali dati non sono o non sono più necessari per il fine per cui erano stati trasmessi o resi disponibili.

8. Se i dati personali sono stati trasmessi senza essere stati richiesti, l'autorità ricevente verifica immediatamente se tali dati sono necessari per il fine per il quale sono stati trasmessi.

9. I dati personali non vengono cancellati ma bloccati conformemente al diritto nazionale se vi sono motivi ragionevoli per credere che tale cancellazione possa compromettere gli interessi legittimi della persona cui si riferiscono i dati. I dati bloccati possono essere utilizzati o trasmessi solo per lo scopo per il quale non sono stati cancellati.

Articolo 10
Registrazione e documentazione

1. Gli Stati membri dispongono affinché qualsiasi trasmissione automatica di dati personali, segnatamente mediante accesso diretto automatico, venga registrata al fine di garantire la successiva verifica dei motivi della trasmissione, dei dati trasmessi, del momento in cui sono stati trasmessi, delle autorità coinvolte e, per quanto riguarda l'autorità ricevente, delle persone che hanno ricevuto i dati e delle persone che ne avevano fatto richiesta.

2. Gli Stati membri dispongono affinché sia documentata qualsiasi trasmissione e ricevimento non automatici di dati personali al fine di garantire la successiva verifica

dei motivi della trasmissione, dei dati trasmessi, del momento in cui sono stati trasmessi, delle autorità coinvolte e, per quanto riguarda l'autorità ricevente, delle persone che hanno ricevuto i dati e delle persone che ne avevano fatto richiesta.

3. L'autorità che ha registrato o documentato tali informazioni è tenuta a comunicarle immediatamente alle autorità competenti di controllo su richiesta di queste ultime. Le informazioni devono essere utilizzate solo per il controllo della protezione dei dati e per garantire un trattamento corretto dei dati nonché l'integrità e la sicurezza di questi.

SEZIONE II – ULTERIORE TRATTAMENTO, SEGNATAMENTE ULTERIORE TRASMISSIONE E TRASFERIMENTO, DEI DATI RICEVUTI O RESI DISPONIBILI DALLE AUTORITÀ COMPETENTI DEGLI ALTRI STATI MEMBRI

Articolo 11
Ulteriore trattamento dei dati personali ricevuti o resi disponibili dalle autorità competenti di un altro Stato membro

1. Gli Stati membri dispongono che, conformemente alla presente decisione quadro e segnatamente agli articoli 4, 5 e 6, il trattamento dei dati personali ricevuti o resi disponibili dalle autorità competenti di un altro Stato membro possa essere effettuato soltanto

   (a) per il fine specifico per il quale sono stati trasmessi o resi disponibili

   (b) se necessario ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali o ai fini della prevenzione di minacce alla sicurezza pubblica o a una persona, tranne che nei casi in cui su tali considerazioni prevalga la necessità di tutelare gli interessi o i diritti fondamentali delle persone cui i dati si riferiscono.

2. Il trattamento ulteriore dei dati personali interessati può essere effettuato per le finalità di cui al paragrafo 1, lettera b) del presente articolo solo previo consenso dell'autorità che ha trasmesso o reso disponibili i dati personali.

3. Il paragrafo 1, lettera b) non si applica nei casi in cui una legislazione specifica adottata in virtù del titolo VI del trattato sull'Unione europea disponga esplicitamente che un ulteriore trattamento dei dati personali ricevuti o resi disponibili dall'autorità competente di un altro Stato membro possa essere effettuato solo per le finalità per la quali tali dati sono stati trasmessi o resi disponibili.

Articolo 12
Trasmissione ad altre autorità competenti

Gli Stati membri dispongono affinché i dati personali ricevuti o resi disponibili dall'autorità competente di un altro Stato membro possano essere trasmessi o resi disponibili ad altre autorità competenti di uno Stato membro solo se sono soddisfatte le seguenti condizioni:

(a) la trasmissione o la messa a disposizione è prevista da una legge che la imponga chiaramente come un obbligo o la autorizzi;

(b) la trasmissione o la messa a disposizione è necessaria per l'adempimento dei compiti legittimi dell'autorità che ha ricevuto i dati in questione o dell'autorità a cui saranno successivamente trasmessi;

(c) la trasmissione o la messa a disposizione è necessaria per il fine specifico per il quale sono stati trasmessi o resi disponibili o ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali o ai fini della prevenzione di minacce alla sicurezza pubblica o a una persona, tranne che nei casi in cui su tali considerazioni prevalga la necessità di tutelare gli interessi o i diritti fondamentali delle persone cui i dati si riferiscono;

(d) l'autorità competente dello Stato membro che ha trasmesso o reso disponibile i dati in questione alle autorità competenti che intendono trasmetterli ulteriormente o renderli disponibili ha dato preventivamente il proprio consenso ad un'ulteriore trasmissione o messa a disposizione.

Articolo 13
Trasmissione ad autorità diverse dalle autorità competenti

Gli Stati membri dispongono affinché i dati personali ricevuti o resi disponibili dall'autorità competente di un altro Stato membro possano essere ulteriormente trasmessi o resi disponibili ad autorità diverse dalle autorità competenti di uno Stato membro solo in casi specifici e se sono soddisfatte tutte le seguenti condizioni:

(a) la trasmissione è prevista da una legge che la imponga chiaramente come un obbligo o la autorizzi;

(b) la trasmissione è

necessaria per il fine specifico per il quale i dati sono stati trasmessi o resi disponibili o ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali o ai fini della prevenzione di minacce alla sicurezza pubblica o a una persona, tranne che nei casi in cui su tali considerazioni prevalga la necessità di tutelare gli interessi o i diritti fondamentali delle persone cui i dati si riferiscono;

oppure

necessaria perché i dati in questione sono indispensabili all'autorità a cui i dati devono essere ulteriormente trasmessi per permetterle di svolgere i propri legittimi compiti e a condizione che la finalità della raccolta o del trattamento che deve essere effettuato da tale autorità non sia incompatibile con il trattamento originario e che gli obblighi giuridici dell'autorità competente che intende trasmettere i dati non vi si oppongano;

oppure

è, indubbiamente, nell'interesse della persona cui i dati si riferiscono e tale persona ha acconsentito ad essa o le circostanze sono tali da far presumere inequivocabilmente tale consenso;

(c) L'autorità competente dello Stato membro che ha trasmesso o reso disponibili i dati in questione alle autorità competenti che intendono trasmetterli ulteriormente ha dato preventivamente il proprio consenso ad una loro ulteriore trasmissione.

Articolo 14
Trasmissione a privati

Gli Stati membri, fatte salve le norme procedurali nazionali in materia penale, dispongono affinché i dati personali ricevuti dalle autorità competenti di un altro Stato membro o da esse resi disponibili possano essere ulteriormente trasmessi a privati di uno Stato membro solo in casi particolari e se sono soddisfatte tutte le condizioni seguenti:

(a) la trasmissione è prevista da una legge che la imponga chiaramente come un obbligo o la autorizzi,

(b) la trasmissione è necessaria per il fine per il quale i dati sono stati trasmessi o resi disponibili o ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali o ai fini della prevenzione di minacce alla sicurezza pubblica o a una persona, tranne che nei casi in cui su tali considerazioni prevalga la necessità di tutelare gli interessi o i diritti fondamentali delle persone cui i dati si riferiscono,

(c) l'autorità competente dello Stato membro che ha trasmesso o reso disponibili i dati in questione alle autorità competenti che intendono trasmetterli ulteriormente ha dato preventivamente il proprio consenso ad una loro ulteriore trasmissione a privati.

Articolo 15
Trasferimento alle autorità competenti di paesi terzi o a organismi internazionali

1. Gli Stati membri dispongono affinché i dati personali ricevuti o resi disponibili dall'autorità competente di un altro Stato membro non possano essere ulteriormente trasferiti alle autorità competenti di paesi terzi o a organismi internazionali tranne che nel caso in cui tale trasferimento sia conforme alla decisione quadro e, segnatamente, siano soddisfatte tutte le seguenti condizioni.

(a) Il trasferimento è previsto da una legge che lo imponga chiaramente come un obbligo o lo autorizzi.

(b) Il trasferimento è necessario per il fine per il quale i dati sono stati trasmessi o resi disponibili o ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali o ai fini della prevenzione di minacce alla sicurezza pubblica o a una persona, tranne che nei casi in cui su tali considerazioni prevalga la necessità di tutelare gli interessi o i diritti fondamentali delle persone cui i dati si riferiscono.

(c) L'autorità competente dell'altro Stato membro che ha trasmesso o reso disponibili i dati in questione alle autorità competenti che intendono trasferirli ulteriormente ha dato preventivamente il proprio consenso ad un loro ulteriore trasferimento.

(d) Il paese terzo o l'organismo internazionale a cui i dati in questioni sono trasferiti garantiscono un adeguato livello di protezione dei dati.

2. Gli Stati membri garantiscono che l'adeguatezza del livello di protezione offerto da un paese terzo o da un organismo internazionale sia valutata alla luce di tutte le circostanze per ciascun trasferimento o categoria di trasferimenti. In particolare, tale valutazione deve avvenire sulla base dei seguenti elementi: il tipo di dati, le finalità e la durata del trattamento per il quale i dati sono trasferiti, il paese di origine e quello di destinazione finale, le norme generali e settoriali del diritto applicabile nel paese terzo o organismo in questione, le norme professionali e di sicurezza ivi applicabili e l'esistenza di garanzie sufficienti fornite dal destinatario del trasferimento.

3. Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo o un organismo internazionale non garantisce un livello di protezione adeguato ai sensi del paragrafo 2.

4. Qualora si accerti, sulla base della procedura prevista dall'articolo 16, che un paese terzo o un organismo internazionale non garantisce un livello adeguato di protezione ai sensi del paragrafo 2, gli Stati membri prendono le misure necessarie per impedire qualsiasi trasferimento di dati personali al paese terzo o organismo internazionale in questione.

5. Conformemente alla procedura di cui all'articolo 16, può essere deciso che un paese terzo o un organismo internazionale garantisce un adeguato livello di protezione ai sensi del paragrafo 2 in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, ai fini della tutela della vita privata o delle libertà e dei diritti dell'individuo.

6. In via eccezionale, i dati personali ricevuti dalle autorità competenti di un altro Stato membro possono essere ulteriormente trasferiti alle autorità competenti di paesi terzi o di organismi internazionali in cui non è garantito un adeguato livello di protezione dei dati se ciò è assolutamente necessario per salvaguardare gli interessi di uno Stato membro o per prevenire gravi pericoli imminenti che minacciano la sicurezza pubblica o una persona o più persone specifiche.

Articolo 16
Comitato

1. Qualora sia fatto riferimento al presente articolo, la Commissione è assistita da un comitato composto dai rappresentanti degli Stati membri e presieduto dal rappresentante della Commissione.

2. Il comitato adotta il proprio regolamento interno su proposta del presidente, basandosi su un modello di regolamento interno pubblicato nella Gazzetta ufficiale dell'Unione europea.

3. Il rappresentante della Commissione sottopone al comitato un progetto delle misure da adottare. Il comitato esprime il suo parere sul progetto entro un termine che il presidente può fissare in funzione dell'urgenza della questione in esame. Il parere deve essere espresso a maggioranza, secondo quando stabilito dall'articolo 205, paragrafo 2 del trattato che istituisce la Comunità europea, nel caso delle decisioni che il Consiglio è tenuto ad adottare su proposta della Commissione. I voti dei rappresentanti degli Stati membri nell'ambito del comitato sono ponderati secondo i criteri che figurano a tale articolo. Il presidente non partecipa al voto.

4. La Commissione adotta le misure previste qualora siano conformi al parere del comitato. Se le misure previste non sono conformi al parere del comitato, o in assenza di parere, la Commissione sottopone senza indugio al Consiglio una proposta in merito alle misure da prendere e ne informa il Parlamento europeo.

5. Il Consiglio può deliberare a maggioranza qualificata entro due mesi dalla data in cui gli è stata presentata la proposta.

   Se entro tale termine il Consiglio ha manifestato a maggioranza qualificata la sua opposizione alla proposta, la Commissione la riesamina. Essa può presentare al Consiglio una proposta modificata, ripresentare la proposta ovvero presentare una proposta legislativa. Se allo scadere di tale termine il Consiglio non ha adottato l'atto di esecuzione proposto ovvero non ha manifestato opposizione alla proposta di misure di esecuzione, la Commissione adotta l'atto di esecuzione proposto.

Articolo 17
Deroghe agli articoli 12, 13, 14 e 15

Gli articoli 12, 13, 14 e 15 non si applicano nei casi in cui una legislazione specifica adottata in virtù del titolo VI del trattato sull'Unione europea disponga esplicitamente che i dati personali ricevuti o resi disponibili dall'autorità competente di un altro Stato membro non possano essere ulteriormente trasmessi o possano essere ulteriormente trasmessi soltanto a determinate condizioni.

Articolo 18
Informazioni su richiesta delle autorità competenti

Gli Stati membri dispongono affinché le autorità competenti cui i dati sono trasmessi o resi disponibili o che trasmettono e rendono disponibili i dati siano informate, quando lo richiedono, sull'ulteriore trattamento dei dati e sui risultati raggiunti.

CAPITOLO IV

DIRITTI DELL'INTERESSATO

Articolo 19
Diritto all'informazione nei casi in cui la raccolta dei dati viene effettuata presso l'interessato e quest'ultimo ne è a conoscenza

1. Gli Stati membri dispongono che il responsabile del trattamento, o il suo rappresentante, debba fornire gratuitamente alla persona presso la quale effettua la raccolta dei dati che la riguardano e che è a conoscenza di tale raccolta almeno le informazioni elencate qui di seguito, a meno che tale persona ne sia già informata:

   (a) l'identità del responsabile del trattamento ed eventualmente del suo rappresentante;

   (b) le finalità del trattamento cui sono destinati i dati;

   (c) ulteriori informazioni riguardanti quanto segue:

   – la base giuridica del trattamento,

   – i destinatari o le categorie di destinatari dei dati;

   – il carattere obbligatorio o facoltativo delle risposte alle domande o di altre forme di cooperazione, nonché le possibili conseguenze di una mancata risposta o di una mancata cooperazione;

   – l'esistenza di diritti di accesso e di rettifica in merito ai dati che riguardano l'interessato;

   nella misura in cui, in considerazione delle specifiche circostanze in cui i dati vengono raccolti, tali informazioni siano necessarie per effettuare un trattamento che sia corretto nei confronti della persona interessata.

2. La fornitura delle informazioni di cui al paragrafo 1 è rifiutata o limitata solo se ciò di rivela necessario per

   (a) permettere al responsabile del controllo di svolgere correttamente i propri compiti,

   (b) non compromettere le indagini, inchieste o procedimenti in corso o lo svolgimento dei legittimi doveri delle autorità competenti,

   (c) tutelare la sicurezza pubblica e l'ordine pubblico negli Stati membri,

   (d) proteggere i diritti e le libertà di terzi,

tranne quando su tali considerazioni prevalga la necessità di tutelare gli interessi o i diritti fondamentali dell'interessato.

3. Qualora le informazioni di cui al paragrafo 1 siano rifiutate o limitate, il responsabile del controllo informa l'interessato che può ricorrere alle autorità di controllo competenti, fatti salvi i ricorsi giurisdizionali e le procedure penali nazionali.

4. I motivi che giustificano un rifiuto o una limitazione ai sensi del paragrafo 2 non vengono forniti se la loro comunicazione pregiudica la finalità del rifiuto. In tal caso, il responsabile del controllo informa l'interessato che può presentare ricorso alle autorità di controllo competenti, fatti salvi i ricorsi giurisdizionali e le procedure penali nazionali. Se l'interessato presenta un ricorso all'autorità di controllo, quest'ultima è tenuta ad esaminarlo. Quando esamina il ricorso, l'autorità di controllo deve soltanto comunicare all'interessato se il trattamento dei dati è stato effettuato correttamente e, in caso contrario, se sono state apportate le opportune modifiche.

Articolo 20
Diritto di informazione nei casi in cui i dati non sono stati ottenuti dall'interessato o sono stati ottenuti da esso senza che ne fosse a conoscenza

1. Qualora i dati non siano stati ottenuti dall'interessato o siano stati ottenuti da esso senza che ne fosse a conoscenza o senza che egli fosse consapevole del fatto che i dati raccolti lo riguardavano, gli Stati membri dispongono affinché il responsabile del controllo o il suo rappresentante comunichi gratuitamente, quando vengono registrati dati personali o entro un tempo ragionevole dal momento in cui dati sono stati comunicati per la prima volta, all'interessato almeno le seguenti informazioni, tranne che nei casi in cui l'interessato ne sia già in possesso o in cui fornire tali informazioni si dimostri impossibile o sproporzionatamente difficile.

   (a) l'identità del responsabile del trattamento ed eventualmente del suo rappresentante;

   (b) le finalità del trattamento,

   (c) ulteriori informazioni riguardanti quanto segue:

   – la base giuridica del trattamento,

   – le categorie di dati interessate,

   – i destinatari o le categorie di destinatari dei dati,

   – se esiste un diritto di accesso ai dati e di rettifica in merito ai dati che lo riguardano,

   nella misura in cui, in considerazione delle specifiche circostanze in cui i dati vengono raccolti, tali informazioni siano necessarie per effettuare un trattamento leale nei confronti della persona interessata.

2. Le informazioni di cui al paragrafo 1 non sono fornite se ciò è necessario per:

(a) permettere al responsabile del controllo di svolgere correttamente i propri compiti,

(b) non compromettere le indagini, inchieste o procedimenti in corso o lo svolgimento dei legittimi doveri delle autorità competenti,

(c) tutelare la sicurezza pubblica e l'ordine pubblico negli Stati membri,

(d) proteggere i diritti e le libertà di terzi,

tranne quando su tali considerazioni prevalga la necessità di tutelare gli interessi o i diritti fondamentali dell'interessato.

Articolo 21
Diritto di accesso, rettifica, cancellazione o blocco

1. Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento:

(a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi:

– la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatari cui sono stati comunicati i dati;

– la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati;

(b) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente decisione quadro, in particolare a causa del carattere incompleto o inesatto dei dati;

(c) la notificazione a terzi, ai quali sono stati comunicati i dati, di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato.

2. Qualsiasi azione che l'interessato ha il diritto di effettuare conformemente al paragrafo 1 è rifiutata se ciò è necessario per:

(a) permettere al responsabile del controllo di svolgere correttamente i propri compiti,

(b) non compromettere le indagini, inchieste o procedimenti in corso o lo svolgimento dei legittimi doveri delle autorità competenti,

(c) tutelare la sicurezza pubblica e l'ordine pubblico negli Stati membri,

(d) proteggere i diritti e le libertà di terzi,

tranne quando su tali considerazioni prevalga la necessità di tutelare gli interessi o i diritti fondamentali dell'interessato.

3. Qualsiasi rifiuto o limitazione dei diritti di cui al paragrafo 1 deve essere formulato per iscritto. Qualora al diritto di cui al paragrafo 1 venga opposto un rifiuto o imposta una limitazione, il responsabile del controllo informa l'interessato che può ricorrere alle autorità di controllo competenti, fatti salvi i ricorsi giurisdizionali e le procedure penali nazionali.

4. I motivi che giustificano un rifiuto ai sensi del paragrafo 2 non vengono forniti se la loro comunicazione pregiudica la finalità del rifiuto. In tal caso, il responsabile del controllo informa l'interessato che può presentare ricorso alle autorità di controllo competenti, fatti salvi i ricorsi giurisdizionali e le procedure penali nazionali. Se l'interessato presenta un ricorso all'autorità di controllo, quest'ultima è tenuta ad esaminarlo. Quando esamina il ricorso, l'autorità di controllo deve soltanto comunicare all'interessato se il trattamento dei dati è stato effettuato correttamente e, in caso contrario, se sono state apportate le opportune modifiche.

Articolo 22
Informazioni a terzi a seguito di una rettifica, blocco o cancellazione

Gli Stati membri dispongono affinché vengano prese misure adeguate per garantire che, nei casi in cui il responsabile del controllo rettifichi, blocchi o cancelli dati personali a seguito di una richiesta, venga elaborato automaticamente un elenco dei fornitori e dei destinatari di tali dati. Il responsabile del controllo è tenuto a garantire che le persone presenti in tale elenco vengano informate dei cambiamenti effettuati riguardo ai dati personali.

CAPITOLO V

Riservatezza e sicurezza del trattamento

Articolo 23
Riservatezza

L'incaricato del trattamento o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento non deve elaborare i dati personali ai quali ha accesso, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi giuridici. Tutti coloro che lavorano con un'autorità competente di uno Stato membro o al suo interno sono vincolati da norme severe di riservatezza.

Articolo 24
Sicurezza

1. Gli Stati membri dispongono affinché il responsabile del controllo prenda misure tecniche ed organizzative adeguate per proteggere i dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla divulgazione o

accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete o la loro messa a disposizione mediante l'assicurazione di un accesso diretto automatico e da qualsiasi altra forma illecita di trattamento di dati personali, segnatamente in relazione ai rischi che il trattamento comporta e alla natura dei dati personali da proteggere.

Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere. Le misure sono considerate necessarie quando l'impegno che esse comportano non è sproporzionato all'obiettivo di protezione.

2. Ciascuno Stato membro adotta, per il trattamento automatizzato dei dati misure atte a:

(a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento di dati di carattere personale (controllo dell'accesso alle attrezzature),

(b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate (controllo dei supporti di dati);

(c) impedire che nell'archivio siano inseriti, senza autorizzazione, dati di carattere personale e che di essi sia presa visione, o che siano modificati o cancellati senza autorizzazione (controllo della memorizzazione);

(d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato di dati mediante attrezzature per la trasmissione di dati (controllo dell'utilizzazione);

(e) garantire che le persone autorizzate ad usare un sistema di elaborazione automatizzata di dati abbiano accesso solo ai dati cui si riferisce la loro autorizzazione d'accesso (controllo dell'accesso ai dati);

(f) garantire che sia possibile verificare ed accertare a quali organizzazioni siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati (controllo dell'utilizzazione);

(g) garantire la possibilità di verificare ed accertare a posteriori quali dati di natura personale sono stati introdotti nei sistemi di trattamento automatizzato di dati, il momento dell'inserimento e la persona che lo ha effettuato (controllo dell'introduzione);

(h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati da persone non autorizzate durante i trasferimenti di dati personali o il trasporto di supporti di dati (controllo del trasporto);

(i) garantire che, in caso di guasto, i sistemi utilizzati possano essere ripristinati immediatamente (riparazione);

(j) garantire che le funzioni del sistema non siano difettose, che eventuali errori di funzionamento siano segnalati immediatamente (affidabilità) e che i dati

memorizzati non possano essere falsati da un errore di funzionamento del sistema (autenticità).

3. Gli Stati membri dispongono che il responsabile del trattamento, quando quest'ultimo sia eseguito per suo conto, deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare e deve assicurarsi del rispetto di tali misure.

4. L'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente:

– che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento,

– che gli obblighi di cui ai paragrafi 1 e 2, quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo.

5. A fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati e i requisiti concernenti le misure di cui al paragrafo 1 sono stipulati per iscritto o in altra forma equivalente.

Articolo 25
Registro

1. Gli Stati membri dispongono che il responsabile del trattamento tenga un registro di tutte le operazioni destinate al conseguimento di una o più finalità correlate. Le informazioni contenute nel registro devono comprendere:

(a) il nome e l'indirizzo del responsabile del trattamento e, eventualmente, del suo rappresentante;

(b) la o le finalità del trattamento;

(c) una descrizione della o delle categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime;

(d) la base giuridica del trattamento al quale sono destinati i dati;

(e) i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;

(f) i trasferimenti di dati previsti verso paesi terzi;

(g) una descrizione generale che consenta una prima valutazione dell'adeguatezza delle misure adottate in virtù dell'articolo 24 per garantire la sicurezza del trattamento.

2. Gli Stati membri precisano le condizioni e le modalità di notificazione all'autorità di controllo delle informazioni di cui al paragrafo 1.

Articolo 26
Controllo preliminare

1. Gli Stati membri individuano quali sono i trattamenti che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone e controllano che tali trattamenti siano esaminati prima della loro messa in opera.

2. Tali esami preliminari sono effettuati dall'autorità di controllo una volta ricevuta la notificazione del responsabile del trattamento, oppure dalla persona incaricata della protezione dei dati che, nei casi dubbi, deve consultare l'autorità di controllo medesima.

3. Gli Stati membri possono effettuare tale esame anche durante il processo di elaborazione di un provvedimento del Parlamento nazionale, o in base ad un provvedimento fondato su siffatto provvedimento legislativo, in cui si definisce il tipo di trattamento e si stabiliscono appropriate garanzie.

CAPITOLO VIRISCORSI GIURISDIZIONALI E RESPONSABILITÀ

Articolo 27
Mezzi di ricorso

Fatti salvi i ricorsi amministrativi che possono essere presentati, segnatamente dinanzi all'autorità di controllo di cui all'articolo 30, prima che sia adita l'autorità giudiziaria, gli Stati membri stabiliscono il diritto di chiunque a presentare un ricorso giurisdizionale in caso di violazione dei diritti garantitigli dal diritto nazionale applicabile ai sensi della presente decisione quadro al trattamento in questione.

Articolo 28
Responsabilità

1. Gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente decisione quadro abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento. Il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile.

2. Tuttavia, un'autorità competente che ha ricevuto i dati personali da parte di un altro Stato membro è responsabile nei confronti della parte lesa per i danni causati a causa dell'uso di dati imprecisi e non aggiornati. Non può escludere la propria responsabilità giustificandola con il fatto che i dati ricevuti da un'altra autorità erano imprecisi o non aggiornati. Qualora i danni vengano addebitati all'autorità ricevente perché ha utilizzato dati imprecisi trasmessi o resi disponibili dall'autorità competente di un altro Stato membro, quest'ultima deve risarcire completamente l'importo pagato per tali danni dall'autorità ricevente.

Articolo 29
Sanzioni

1. Gli Stati membri adottano le misure appropriate per garantire la piena applicazione delle disposizioni della presente decisione quadro e in particolare stabiliscono sanzioni efficaci, commisurate e dissuasive da applicare in caso di violazione delle disposizioni di attuazione della presente decisione quadro.

2. Gli Stati membri prevedono sanzioni penali efficaci, commisurate e dissuasive per i reati commessi intenzionalmente che comportano violazioni gravi delle disposizioni adottate conformemente alla presente decisione quadro, segnatamente le disposizioni finalizzate a garantire la riservatezza e la sicurezza del trattamento.

CAPITOLO VII

AUTORITÀ DI SORVEGLIANZA E GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Articolo 30
Autorità di sorveglianza

1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente decisione quadro, adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.

2. Ciascuno Stato membro dispone che le autorità di controllo siano consultate al momento dell'elaborazione delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali ai fini della prevenzione, delle indagini e del perseguimento della criminalità e dei reati penali.

3. Ogni autorità di controllo dispone in particolare:

   – di poteri investigativi, come la facoltà di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo,

   – di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 26, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;

   – del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente decisione quadro ovvero di adire per dette violazioni le autorità giudiziarie.

È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.

4. Qualsiasi persona può presentare a un'autorità di controllo una domanda relativa alla tutela dei propri diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda.

5. Ogni autorità di controllo elabora a intervalli regolari una relazione sulle proprie attività. La relazione è oggetto di pubblicazione.

6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro.

7. Le autorità di sorveglianza cooperano tra loro e con le autorità di controllo di cui al titolo VI del trattato sull'Unione europea e con il garante europeo della protezione dei dati nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile.

8. Gli Stati membri dispongono che i membri e il personale delle autorità di controllo sono soggetti, anche dopo la cessazione delle attività, all'obbligo del segreto professionale in merito alle informazioni riservate cui hanno accesso.

9. I poteri dell'autorità di sorveglianza non pregiudicano l'indipendenza dei magistrati e le decisioni prese da tale autorità non pregiudicano l'esercizio delle legittime funzioni dei magistrati nei procedimenti penali.

Articolo 31

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali ai fini della prevenzione, delle indagini, dell'accertamento e del perseguimento dei reati penali

1. È istituito un gruppo di lavoro per la tutela della persone con riguardo al trattamento dei dati personali ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali, in appresso denominato «il gruppo». Il gruppo ha carattere consultivo e indipendente.

2. Il gruppo è composto da un rappresentante della o delle autorità di controllo designate da ciascuno Stato membro e da un rappresentante del garante europeo della protezione dei dati, nonché da un rappresentante della Commissione.

   Ogni membro del gruppo è designato dall'istituzione oppure dalla o dalle autorità che rappresenta. Qualora uno Stato membro abbia designato più autorità di controllo, queste procedono alla nomina di un rappresentante comune.

   I presidenti delle autorità di controllo comuni istituite ai sensi del titolo VI del trattato sull'Unione europea hanno il diritto di partecipare o di essere rappresentati alle riunioni del gruppo di lavoro. L'autorità o le autorità di sorveglianza istituite dall'Islanda, dalla Norvegia e dalla Svizzera hanno il diritto di essere rappresentate alle riunioni del gruppo di lavoro nella misura in cui si trattino questioni legate all'acquis di Schengen.

3. Il gruppo adotta le proprie decisioni alla maggioranza semplice dei rappresentanti delle autorità di controllo degli Stati membri.

4. Il gruppo elegge il proprio presidente. La durata del mandato del presidente è di due anni. Il mandato è rinnovabile.

5. Al segretariato del gruppo provvede la Commissione.

6. Il gruppo adotta il proprio regolamento interno.

7. Il gruppo di lavoro esamina i punti messi all'ordine del giorno dal presidente, di propria iniziativa o su richiesta di un rappresentante di un'autorità di sorveglianza, della Commissione, del garante europeo della protezione dei dati o dei presidenti delle autorità di controllo comuni.

Articolo 32
Funzioni

1. Il gruppo ha i seguenti compiti:

   (a) esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della presente decisione quadro per contribuire alla loro applicazione omogenea,

   (b) fornire un parere sul livello di protezione negli Stati membri e nei paesi terzi ed organismi internazionali, segnatamente al fine di garantire che i dati personali siano trasferiti, conformemente all'articolo 15 della presente decisione quadro, solo ai paesi terzi ed organismi internazionali che garantiscono un livello adeguato di protezione di dati,

   (c) fornire consulenze alla Commissione e agli Stati membri su ogni proposta di modifica della presente decisione quadro o su qualsiasi altra misura supplementare o specifica per tutelare: i diritti e le libertà delle persone fisiche riguardo al trattamento dei dati personali ai fini della prevenzione, delle indagini, dell'accertamento edel perseguimento dei reati penali nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano su tali diritti e libertà.

2. Il gruppo, qualora constati che tra le legislazioni e le prassi degli Stati membri si manifestino divergenze che possono pregiudicare l'equivalenza della tutela delle persone in materia di trattamento dei dati personali nell'Unione europea, ne informa il Consiglio e la Commissione.

3. Il gruppo può, di propria iniziativa o su iniziativa della Commissione o del Consiglio, formulare raccomandazioni su qualsiasi questione riguardante la tutela delle persone relativamente al trattamento di dati personali nell'Unione europea ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali.

4. I pareri e le raccomandazioni del gruppo vengono trasmessi al Consiglio, alla Commissione, al Parlamento e al comitato di cui all'articolo 16.

5. La Commissione, sulla base delle informazioni fornite dagli Stati membri, informa il gruppo sulle azioni intraprese a seguito dei suoi pareri e raccomandazioni. A tal fine redige una relazione che viene trasmessa anche al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione. Gli Stati membri informano il gruppo su qualsiasi azione da essi intrapresa ai sensi del paragrafo 1.

6. Il gruppo redige una relazione annuale sullo stato della tutela delle persone fisiche con riguardo al trattamento dei dati personali ai fini della prevenzione, delle indagini e del perseguimento della criminalità e dei reati penali nell'Unione europea e nei paesi terzi e la trasmette alla Commissione, al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione.

CAPITOLO VIII

Disposizioni finali

Articolo 33
Modifica della convenzione di Schengen

Per le materie che ricadono nell'ambito di applicazione del trattato sull'Unione europea, la presente decisione quadro sostituisce gli articoli 126-130 della convenzione di Schengen.

Articolo 34
Relazione con altri strumenti relativi al trattamento e alla protezione dei dati personali

1. La presente decisione quadro sostituisce l'articolo 23 della convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea.

2. Qualsiasi riferimento alla convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del 28 gennaio 1981 deve essere considerato come un riferimento alla presente decisione quadro.

Articolo 35
Attuazione

1. Gli Stati membri adottano le disposizioni necessarie per conformarsi alla presente decisione quadro entro 31.12.06.

2. Entro tale data gli Stati membri trasmettono al Segretariato generale del Consiglio e alla Commissione il testo delle disposizioni che recepiscono nel diritto nazionale gli obblighi loro imposti dalla presente decisione quadro e le informazioni relative alla nomina dell'autorità di sorveglianza di cui all'articolo 29. Sulla base di tali informazioni e di una relazione scritta della Commissione, il Consiglio valuta, entro il 31 dicembre 2007, in che misura gli Stati membri abbiano adottato le misure necessarie per attuare la presente decisione quadro.

Articolo 36
Entrata in vigore

La presente decisione quadro entra in vigore il ventesimo giorno successivo alla data della pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il […]

Per il Consiglio
Il Presidente

ALLEGATO

SCHEDA FINANZIARIA LEGISLATIVA

Settore(i) politico(i): Giustizia e affari interni

Attività: 1806 – Creazione di un autentico spazio di libertà, sicurezza e giustizia in materia civile e penale

DENOMINAZIONE DELL'AZIONE: PROPOSTA DI DECISIONE QUADRO DEL CONSIGLIO SULLA PROTEZIONE DEI DATI PERSONALI TRATTATI NELL'AMBITO DELLA COOPERAZIONE GIUDIZIARIA E DI POLIZIA IN MATERIA PENALE

1. LINEA(E) DI BILANCIO + DENOMINAZIONE

NA

2. DATI GLOBALI IN CIFRE

2.1. Dotazione finanziaria complessiva per l'azione (Parte B): impegni in milioni di euro

NA

2.2. Periodo di applicazione:

inizio nel 2006

2.3. Stima globale pluriennale delle spese:

(a) Scadenziario stanziamenti d'impegno/stanziamenti di pagamento (intervento finanziario) (*cfr. punto 6.1.1)*

milioni di EUR (*al terzo decimale*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Totale
Stanziamenti di impegno							
Stanziamenti di pagamento							

(b) Assistenza tecnica e amministrativa (ATA) e spese d'appoggio (SDA) (*cfr. punto 6.1.2*)

Stanziamenti di impegno							
Stanziamenti di pagamento							

Totale parziale a + b							
Stanziamenti di impegno							
Stanziamenti di pagamento							

(c) Incidenza finanziaria globale delle risorse umane e di altre spese di funzionamento*(cfr. punti 7.2 e 7.3)*

Impegni/pagamenti	0.389	0.389	0.389	0.389	0.389	0.389	2,334

TOTALE a + b + c							
Stanziamenti di impegno							
Stanziamenti di pagamento							

2.4. Compatibilità con la programmazione finanziaria e le prospettive finanziarie

NA

2.5. Incidenza finanziaria sulle entrate:

Nessuna incidenza finanziaria.

3. CARATTERISTICHE DI BILANCIO

Natura della spesa		**Nuova**	**Contributo EFTA**	**Contributo dei paesi candidati**	**Rubrica delle prospettive finanziarie**
SNO	/SND	NA	NA	NA	No NA

4. BASE GIURIDICA

Articolo 30, 31 e 34, paragrafo 2, lettera b) del TUE

5. DESCRIZIONE E GIUSTIFICAZIONE

5.1. Necessità dell'intervento comunitario

5.1.1. Obiettivi perseguiti

La proposta di decisione quadro prevede norme comuni relative alla protezione dei dati personali trattati dalle autorità competenti nell'ambito delle attività previste dal

titolo VI del trattato sull'Unione europea (cooperazione giudiziaria e di polizia in materia penale). Conformemente alla presente decisione quadro, l'applicazione delle disposizioni nazionali negli Stati membri deve essere controllata da autorità di sorveglianza pubbliche indipendenti. A livello dell'UE è istituito un gruppo per la tutela della persone con riguardo al trattamento dei dati personali ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento dei reati penali, in appresso denominato «il gruppo». Il gruppo è composto da un rappresentante della o delle autorità di controllo designate da ciascuno Stato membro e da un rappresentante del garante europeo della protezione dei dati, nonché da un rappresentante della Commissione. Il gruppo esamina ogni questione attinente all'applicazione delle norme nazionali di attuazione della presente decisione quadro per contribuire alla loro applicazione omogenea. Formula pareri sul livello di protezione dei dati negli Stati membri e nei paesi terzi e fornisce consulenze alla Commissione e agli Stati membri in merito a ogni progetto di modifica della presente decisione quadro nonché a qualsiasi altra misura supplementare o specifica per tutelare i diritti fondamentali.

Inoltre, conformemente all'articolo 16 della presente decisione quadro, la Commissione è assistita da un comitato, composto dai rappresentanti degli Stati membri e presieduto dal rappresentante della Commissione, al fine di valutare, ove necessario, il livello della protezione dei dati in un paese terzo.

5.1.2. Disposizioni adottate in relazione alla valutazione ex-ante

Sono stati consultati i rappresentanti dei Governi e delle autorità indipendenti di sorveglianza degli Stati membri nonché dell'Islanda, della Norvegia e della Svizzera, il garante europeo della protezione dei dati, Europol e Eurojust. In particolare, tenuto conto dei diversi pareri, la Commissione propone di istituire il gruppo di cui sopra. Al fine di calcolare gli eventuali costi determinati da questa misura, la Commissione ha verificato i costi (spese di viaggio, servizi di segretariato per la preparazione e l'organizzazione delle riunioni) attualmente sostenute dal gruppo istituito conformemente all'articolo 29 della direttiva 95/46/CE.

5.2. Azione prevista e modalità dell'intervento di bilancio

Il suddetto gruppo terrà regolarmente delle riunioni che, si calcola, saranno circa cinque all'anno. Il comitato di cui all'articolo 16 si riunirà ogni qualvolta ciò si renda necessario, probabilmente anch'esso cinque volte all'anno. Saranno rimborsate le spese di un partecipante per ciascuno Stato membro e Stato Schengen (Islanda, Norvegia). Alcuni orientamenti si possono acquisire dai gruppi istituiti conformemente agli articoli 29 e 31 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

5.3. Modalità di attuazione

La Commissione organizza e ospita tutte le riunioni. La Commissione provvede ai servizi di segretariato per il gruppo e il comitato di cui sopra e alla preparazione/organizzazione delle loro riunioni.

6. INCIDENZA FINANZIARIA

6.1. Incidenza finanziaria totale sulla parte B (per tutto il periodo di programmazione)

6.1.1. Intervento finanziario

NA

6.1.2. Assistenza tecnica ed amministrativa, spese d'appoggio e spese relative alle tecnologie dell'informazione (stanziamenti d'impegno)

NA

6.2. Calcolo dei costi per misura prevista nella parte B (per tutto il periodo di programmazione)

NA

7. INCIDENZA SULLE SPESE DI PERSONALE E AMMINISTRATIVE

L'incidenza sulle spese di personale e amministrative è coperta dalle risorse della DG preposta alla gestione nell'ambito della procedura di assegnazione annuale.

L'assegnazione dei posti dipende anche dall'attribuzione delle funzioni e delle risorse nel contesto delle prospettive finanziarie 2007-2013.

7.1. Incidenza sulle risorse umane

Tipi di posto		Personale da assegnare alla gestione dell'azione usando risorse esistenti e/o supplementari		Totale	Descrizione dei compiti inerenti all'azione
		Numero di posti permanenti	Numero di posti temporanei		
Funzionari o personale temporaneo	A B C	0,25 A 0,50 B 1,00 C		0,25A 0,50B 1,00C	Servizi di segretariato per la preparazione delle riunioni del gruppo di lavoro e del comitato
Altre risorse umane					
Totale					

7.2. Incidenza finanziaria globale delle risorse umane

Tipo di risorsa umana	Importo (EUR)	Modo di calcolo *
Funzionari Personale temporaneo	I anno189. 000	1 X 108 000 0,5 X 108 000 0,25 X 108 000 = 189 .000

Altre risorse umane (indicare la linea di bilancio)		
Totale	189.000	

Gli importi corrispondono alla spesa totale per dodici mesi.

7.3. Altre spese amministrative derivanti dall'azione

Linea di bilancio (numero e denominazione)	Importi in EUR	Modo di calcolo
Dotazione globale (titolo A7) A0701 – Missioni A07030 – Riunioni A07031 - Comitati obbligatori A07032 - Comitati non obbligatori A07040 – Conferenze A0705 - Studi e consulenze Altre spese (specificare)	200.000	10 riunioni*27*740 EUR
Sistemi di informazione (A-5001/A-4300)		
Altre spese - parte A (specificare)		
Totale	200.000	

Gli importi corrispondono alla spesa totale per dodici mesi.

Specificare il tipo di comitato e il gruppo al quale appartiene.

I.	Totale annuale (7.2 + 7.3)	€389.000
II.	Durata dell'azione	
III.	Costo totale dell'azione (I x II)	

8. CONTROLLO E VALUTAZIONE

8.1. Sistema di controllo

Il gruppo di lavoro e il comitato stabiliscono il loro regolamento interno che prevede anche norme in materia di riservatezza. Il Parlamento europeo è informato analogamente a quanto previsto dall'articolo 7 della decisione del Consiglio

99/468/CE del 28.6.1999 recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione (GU L 184 del 17.7.1999, pag. 23).

8.2. Modalità e periodicità della valutazione

NA

9. MISURE ANTIFRODE

NA

XXX