

## PARERI

## GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

**Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio — «La politica antiterrorismo dell'UE: principali risultati e sfide future»**

(2011/C 56/02)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare gli articoli 7 e 8,

vista 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 libera circolazione di tali dati <sup>(1)</sup>,

visto il 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 <sup>(2)</sup>, in particolare l'articolo 41,

HA ADOTTATO IL SEGUENTE PARERE:

## I. INTRODUZIONE

1. Il 20 luglio 2010 la Commissione ha adottato una comunicazione dal titolo «La politica antiterrorismo dell'UE: principali risultati e sfide future» <sup>(3)</sup>. La comunicazione intende fornire «gli elementi fondamentali per una valutazione politica dell'attuale strategia antiterrorismo dell'UE» e costituisce inoltre un elemento della strategia di sicurezza interna <sup>(4)</sup>. Valuta i risultati conseguiti e delinea sfide e orientamenti politici futuri per la politica antiterrorismo dell'UE.

<sup>(1)</sup> GU L 281 del 23.11.1995, pag. 31.

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

<sup>(3)</sup> COM(2010) 386 definitivo.

<sup>(4)</sup> Cfr. la pagina 2 della comunicazione.

2. Molte delle iniziative indicate nella comunicazione sono già state oggetto di osservazioni o pareri specifici del GEPD. Questa comunicazione, tuttavia, presenta un'ampia prospettiva politica e orientamenti a lungo termine che giustificano un parere dedicato del GEPD.

3. Il presente parere intende pertanto contribuire alla formulazione di scelte politiche più fondamentali in un settore in cui l'utilizzo delle informazioni personali è al tempo stesso cruciale, massiccio e particolarmente sensibile.

4. Il parere non formula raccomandazioni sulla più recente comunicazione elaborata dalla Commissione in questo settore, «La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura», adottata il 22 novembre 2010 <sup>(5)</sup>. Questa comunicazione verrà analizzata dal GEPD in un parere separato che inoltre affronterà nuovamente la necessità di istituire collegamenti chiari tra i vari documenti.

5. Nel presente parere il GEPD analizza i diversi elementi della comunicazione, fornendo al contempo consulenza e raccomandazioni volte a garantire il rispetto del diritto fondamentale alla protezione dei dati personali nel settore della politica antiterrorismo dell'UE, specialmente quando si tratta di affrontare sfide future e sviluppare nuovi orientamenti politici.

## II. ANALISI DELLA COMUNICAZIONE E QUESTIONI RELATIVE ALLA PROTEZIONE DEI DATI

6. Basandosi sulla struttura della strategia antiterrorismo dell'Unione europea del 2005 <sup>(6)</sup>, la comunicazione analizza innanzitutto i quattro settori d'azione principali della politica antiterrorismo dell'UE: prevenzione, protezione, perseguimento e risposta. Un capitolo specifico affronta quindi alcune questioni orizzontali, ossia il rispetto dei diritti fondamentali, la cooperazione internazionale e il finanziamento.

<sup>(5)</sup> COM(2010) 673 definitivo.

<sup>(6)</sup> Doc. 14469/4/05 del 30 novembre 2005.

### 1. Prevenzione, protezione, perseguimento, risposta e necessità di integrare i principi di protezione dei dati

7. La «prevenzione» comprende una vasta serie di attività, volte non solo a prevenire la radicalizzazione e il reclutamento, ma anche ad affrontare il modo in cui i terroristi usano Internet. Tra i principali risultati conseguiti in quest'ambito, la comunicazione cita la decisione quadro del Consiglio sulla lotta contro il terrorismo, adottata nel 2002 <sup>(1)</sup> e modificata nel 2008 <sup>(2)</sup>.
8. Anche la «protezione» delle persone e delle infrastrutture è una questione molto ampia, che comprende iniziative in materia di sicurezza alle frontiere, sicurezza dei trasporti, controllo di precursori di esplosivi, protezione delle infrastrutture critiche e rafforzamento della catena di approvvigionamento.
9. Tra le attività di «perseguimento» figurano la raccolta delle informazioni, la cooperazione di polizia e giudiziaria, il contrasto delle attività terroristiche e la lotta contro il finanziamento del terrorismo. Le sfide future in questo settore sono la definizione di un quadro UE sui dati del codice di prenotazione (PNR) <sup>(3)</sup>, l'utilizzo dell'articolo 75 TFUE quale base giuridica per l'elaborazione di una serie di misure finalizzate al congelamento dei capitali e dei beni finanziari nonché il principio del reciproco riconoscimento nell'assunzione delle prove in materia penale.
10. Le attività di «risposta» si riferiscono alla capacità di far fronte alle conseguenze di un attentato terroristico e comprendono l'assistenza alle vittime del terrorismo.
11. Tutti questi settori presentano forti legami con iniziative su cui il GEPD ha già assunto una posizione: il programma di Stoccolma, misure restrittive e congelamento dei beni, conservazione dei dati, body scanner, precursori di armi, dati biometrici, la decisione Prüm, i dati del codice di prenotazione (PNR), l'accordo TFTP (programma di controllo delle transazioni finanziarie dei terroristi), il sistema di informazione Schengen, il sistema di informazione visti, la gestione integrata delle frontiere, la strategia di gestione delle informazioni dell'UE e lo scambio transfrontaliero di prove.
12. I settori della «prevenzione» e della «protezione» sono i più delicati dal punto di vista della protezione dei dati per una serie di motivi.
13. Innanzi tutto, questi settori si basano, per definizione, su valutazioni prospettiche dei rischi che nella maggior parte dei casi implicano un trattamento ampio e «preventivo» di enormi quantità di dati personali su cittadini non sospettati (quali, ad esempio, screening di Internet, frontiere elettroniche e body scanner).
14. In secondo luogo, la comunicazione prevede un rafforzamento dei partenariati tra autorità di contrasto e imprese private (quali fornitori di servizi Internet, istituti finanziari e società di trasporto) finalizzato a favorire lo scambio di informazioni pertinenti e talvolta a «delegare» loro talune parti dei compiti di contrasto. Ciò comporta un maggiore utilizzo dei dati personali, raccolti da imprese private a fini commerciali, da parte delle autorità pubbliche a fini di contrasto.
15. Molte di queste iniziative sono state spesso adottate per fornire una risposta rapida ad azioni terroristiche, senza effettuare un esame approfondito di eventuali duplicazioni o sovrapposizioni con misure già esistenti. In talune circostanze, anche ad alcuni anni di distanza dalla loro entrata in vigore, non è ancora stato possibile stabilire in quale misura l'intrusione nella vita privata dei cittadini derivante da queste misure sia stata effettivamente necessaria in tutti i casi.
16. Esistono inoltre maggiori probabilità che l'utilizzo «preventivo» dei dati personali dia luogo a discriminazioni. L'analisi preventiva delle informazioni comporterebbe la raccolta e il trattamento di dati personali riguardanti ampie categorie di persone (ad esempio tutti i passeggeri, tutti gli utenti di Internet) a prescindere dall'esistenza di sospetti specifici nei loro confronti. L'analisi di queste informazioni, specialmente se associata a tecniche di estrazione dei dati, potrebbe determinare la segnalazione di persone innocenti come individui sospetti solo perché il loro profilo (età, sesso, religione eccetera) e/o i loro schemi (ad esempio di viaggio, di utilizzo di Internet eccetera) coincidono con quelli di persone legate al terrorismo o sospettate di essere implicate in attività terroristiche. Di conseguenza, specialmente in questo contesto, un uso illecito o improprio di informazioni personali (talvolta sensibili), associato agli ampi poteri coercitivi delle autorità di contrasto, può comportare la discriminazione e la stigmatizzazione di persone e/o gruppi di persone specifici.
17. In quest'ottica, garantire un livello elevato di protezione dei dati è inoltre un modo per favorire la lotta contro il razzismo, la xenofobia e la discriminazione, che, secondo la comunicazione, può «anche contribuire a prevenire la radicalizzazione e il reclutamento nelle fila del terrorismo».

### 2. Un approccio coerente basato sul principio di necessità

18. Un'osservazione generale importante riguarda la necessità di garantire coerenza e relazioni chiare tra tutte le comunicazioni e le iniziative adottate nel settore degli affari interni e in particolare nel settore della sicurezza interna. Ad esempio, benché la strategia antiterrorismo dell'UE sia strettamente correlata alla strategia di gestione delle informazioni, alla strategia per il rispetto della Carta dei diritti fondamentali e al modello europeo di scambio delle informazioni, le relazioni tra tutti questi documenti non vengono affrontate espressamente ed approfonditamente. «La

<sup>(1)</sup> Decisione quadro del Consiglio 2002/475/GAI, (GU L 164 del 22.6.2002, pag. 3).

<sup>(2)</sup> Decisione quadro del Consiglio 2008/919/GAI, (GU L 330 del 9.12.2008, pag. 21).

<sup>(3)</sup> Come peraltro annunciato nel piano d'azione della Commissione per l'attuazione del programma di Stoccolma COM(2010) 171 definitivo del 20 aprile 2010.

strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura»<sup>(1)</sup>, adottata il 22 novembre 2010, ha ulteriormente evidenziato tale lacuna.

19. Il GEPD raccomanda pertanto alle istituzioni dell'UE di garantire che le politiche e le iniziative adottate nel settore degli affari interni e della sicurezza interna siano concepite e attuate in maniera tale da assicurare un approccio coerente e relazioni chiare tra loro, prevedendo sinergie adeguate e positive ed evitando duplicazioni del lavoro e degli sforzi.
20. Il GEPD raccomanda inoltre di tenere espressamente in considerazione il principio di necessità in tutte le proposte presentate in questo settore. A tale proposito occorre sia considerare eventuali sovrapposizioni con strumenti già esistenti sia limitare la raccolta e lo scambio di dati personali a quanto effettivamente necessario agli scopi perseguiti.
21. Ad esempio, nel caso dell'accordo sul programma di controllo delle transazioni finanziarie dei terroristi (TFTP II) con gli USA, il GEPD aveva messo in discussione la misura in cui l'accordo fosse effettivamente necessario a ottenere risultati che avrebbero potuto essere conseguiti utilizzando strumenti meno invasivi della vita privata, come quelli già previsti dal quadro UE e internazionale esistente<sup>(2)</sup>. Nello stesso parere, il GEPD aveva messo in dubbio la necessità di trasmettere i dati personali in blocco, anziché in maniera più mirata.
22. Tra le sfide segnalate dalla comunicazione figura la necessità di «garantire che questi strumenti rispondano alle reali necessità (di contrasto) assicurando al tempo stesso il pieno rispetto del diritto alla vita privata e delle norme sulla protezione dei dati». Il GEPD accoglie con favore questo riconoscimento esplicito e invita le istituzioni dell'UE a valutare attentamente la misura in cui gli strumenti già esistenti e quelli previsti soddisfano le effettive necessità di contrasto, evitando al contempo sovrapposizioni di misure o inutili limitazioni alla vita privata. In quest'ottica, gli strumenti esistenti dovranno dimostrare di costituire mezzi efficaci di lotta al terrorismo nell'ambito di revisioni periodiche.
23. Il GEPD ha evidenziato in numerosi pareri e osservazioni la necessità di valutare tutti gli strumenti esistenti sullo scambio di informazioni prima di proporre di nuovi, accordando particolare rilievo a questo aspetto nel recente parere sul «Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia»<sup>(3)</sup>. Di fatto, valutare l'efficacia delle misure esistenti tenendo al tempo stesso in considerazione l'impatto sulla vita privata delle nuove misure previste è fondamentale e deve rivestire un ruolo determinante nell'azione dell'Unione europea in questo settore, in linea con l'approccio proposto dal programma di Stoccolma.

24. Sovrapposizioni e inconcludenze dovrebbero determinare adattamenti delle scelte politiche o portare addirittura al consolidamento o all'abbandono dei sistemi di raccolta e trattamento dei dati esistenti.

25. Il GEPD raccomanda di riservare un'attenzione speciale a quelle proposte da cui scaturiscono raccolte generali di dati personali di tutti i cittadini, anziché solo delle persone sospettate. I casi in cui le informazioni personali vengono trattate a fini diversi da quelli per cui erano state raccolte inizialmente, come avviene ad esempio per l'accesso a fini di contrasto ai dati personali registrati nel sistema Eurodac, richiedono un'attenzione speciale e una giustificazione specifica.

26. La comunicazione sottolinea altresì che una delle sfide future sarà garantire un'efficace politica nel settore della ricerca in materia di sicurezza, che contribuirà ad instaurare un elevato livello di sicurezza. Il GEPD sostiene la dichiarazione della comunicazione secondo cui un'efficace ricerca in materia di sicurezza rafforzerà le relazioni tra i differenti attori. In quest'ottica è fondamentale inserire fin dall'inizio le competenze in materia di protezione dei dati nelle attività di ricerca sulla sicurezza in modo tale da orientare le opzioni politiche e garantire la massima integrazione possibile della vita privata nelle nuove tecnologie orientate alla sicurezza, conformemente al principio della «privacy by design» (tutela della vita privata fin dalla progettazione).

### 3. Riguardo all'uso di misure restrittive (congelamento dei beni)

27. Per quanto riguarda l'uso di misure restrittive (congelamento dei beni) nei confronti di paesi specifici e sospetti terroristi, la giurisprudenza della Corte di giustizia ha ripetutamente e costantemente confermato che il rispetto dei diritti fondamentali nella lotta contro il terrorismo riveste un'importanza cruciale, al fine di garantire sia il rispetto dei diritti dei cittadini sia la legittimità dei provvedimenti adottati.

28. Il GEPD ha già fornito il proprio contributo formulando pareri e osservazioni in quest'ambito<sup>(4)</sup>, evidenziando da un lato i progressi compiuti a livello procedurale, ma chiedendo dall'altro di apportare ulteriori miglioramenti,

<sup>(1)</sup> Cfr. il paragrafo 4 del presente parere.

<sup>(2)</sup> Parere del GEPD del 22 giugno 2010.

<sup>(3)</sup> Parere del GEPD del 30 settembre 2010.

<sup>(4)</sup> Parere del 28 luglio 2009 sulla proposta di regolamento del Consiglio recante modifica del regolamento (CE) n. 881/2002 che impone specifiche misure restrittive nei confronti di determinate persone ed entità associate a Osama bin Laden, alla rete Al-Qaeda e ai Talebani, (GU C 276 del 17.11.2009, pag. 1). Parere del 16 dicembre 2009 su varie proposte legislative che impongono determinate misure restrittive specifiche nei confronti di Somalia, Zimbabwe, Repubblica democratica di Corea e Guinea, (GU C 73 del 23.3.2010, pag. 1). Cfr. anche la lettera del GEPD del 20 luglio 2010 su tre proposte legislative riguardanti talune misure restrittive, segnatamente nei confronti di Milosevic e delle persone a lui collegate, a sostegno del mandato del Tribunale penale internazionale per l'ex Jugoslavia e nei confronti dell'Eritrea. Tutti i pareri e le osservazioni del GEPD sono disponibili sul sito Internet del GEPD all'indirizzo: <http://www.edps.europa.eu>

specialmente riguardo al diritto di informazione e di accesso ai dati personali, alla definizione chiara delle restrizioni a tali diritti nonché al diritto a effettivi ricorsi giurisdizionali e a un controllo indipendente.

29. La necessità di apportare ulteriori miglioramenti alle procedure e alle garanzie previste per le persone iscritte nell'elenco del comitato per le sanzioni è stata recentemente confermata dal Tribunale nella cosiddetta causa «Kadi II»<sup>(1)</sup>. In particolare, il Tribunale ha evidenziato la necessità di fornire alla persona iscritta nell'elenco informazioni circostanziate sui motivi che ne hanno determinato la registrazione. Tale riconoscimento risulta molto simile ai diritti, sanciti dalla legislazione in materia di protezione dei dati, di avere accesso ai propri dati personali e di ottenerne la rettifica, in particolare nel caso in cui siano errati o non aggiornati. Tali diritti, espressamente menzionati dall'articolo 8 della Carta dei diritti fondamentali, costituiscono elementi chiave della protezione dei dati e possono essere soggetti a limitazioni solo nella misura in cui tali limitazioni siano necessarie, prevedibili e stabilite dalla legge.
30. In quest'ottica, il GEPD conviene con la comunicazione che una delle sfide future nel settore della politica antiterrorismo sarà l'utilizzo dell'articolo 75 del TFUE. Questa nuova base giuridica, introdotta dal trattato di Lisbona, prevede espressamente l'adozione di misure di congelamento dei beni nei confronti di persone fisiche o giuridiche. Il GEPD raccomanda di utilizzare questa base giuridica anche per definire un quadro per il congelamento dei beni che sia pienamente conforme al rispetto dei diritti fondamentali. Il GEPD è disponibile a contribuire ulteriormente allo sviluppo di procedure e strumenti legislativi pertinenti e auspica di essere opportunamente e tempestivamente consultato quando la Commissione, conformemente al suo programma di lavoro per il 2011, svilupperà un regolamento specifico in questo settore<sup>(2)</sup>.
31. In una prospettiva più ampia, sussiste la necessità di definire un quadro per la protezione dei dati applicabile anche alla politica estera e di sicurezza comune. Di fatto, l'articolo 16 del TFUE fornisce una base giuridica per la definizione di norme in materia di protezione dei dati anche nel settore della politica estera e di sicurezza comune. L'articolo 39 del TUE prevede una base giuridica e una procedura differenti che verranno applicate solo quando saranno gli Stati membri a trattare i dati personali in questo settore. Tuttavia, benché il trattato di Lisbona preveda l'elaborazione di norme in materia di protezione dei dati e fornisca gli strumenti per definirle, finora la recente comunicazione della Commissione su «Un approccio globale alla protezione dei dati personali nell'Unione europea»<sup>(3)</sup> non contempla alcuna iniziativa in tal senso. Di conseguenza, il

GEPD esorta la Commissione a presentare una proposta per la definizione di un quadro per la protezione dei dati nel settore della politica estera e di sicurezza comune.

#### 4. Rispetto dei diritti fondamentali e cooperazione internazionale

32. Il capitolo dedicato al rispetto dei diritti fondamentali sottolinea che l'UE deve dimostrarsi esemplare nel rispetto della Carta dei diritti fondamentali, alla quale devono improntarsi tutte le sue politiche. Il GEPD accoglie con favore questo approccio.
33. Il GEPD sostiene altresì la dichiarazione secondo cui il rispetto dei diritti fondamentali non è solo un obbligo giuridico, ma anche una condizione fondamentale per promuovere la fiducia fra le autorità nazionali e quella dei cittadini in generale.
34. In tale contesto, affinché sia possibile realizzare questo obiettivo, il GEPD raccomanda l'adozione di un approccio proattivo e di azioni concrete, anche quale mezzo per attuare efficacemente la Carta dei diritti fondamentali dell'UE<sup>(4)</sup>.
35. Le valutazioni d'impatto sulla tutela della vita privata e la consultazione tempestiva delle competenti autorità di protezione dei dati devono essere garantite per tutte le iniziative che incidono sulla protezione dei dati personali, a prescindere dal loro promotore e dal settore in cui vengono proposte.
36. Nel capitolo dedicato alla cooperazione internazionale la comunicazione evidenzia altresì la necessità di creare «condizioni giuridiche e politiche necessarie a una cooperazione rafforzata con i partner esterni dell'UE nel campo della lotta contro il terrorismo».
37. A tale proposito il GEPD ricorda la necessità di assicurare l'esistenza di garanzie adeguate per lo scambio di dati personali con i paesi terzi e le organizzazioni internazionali affinché sia possibile garantire che i diritti dei cittadini in materia di protezione dei dati siano opportunamente rispettati anche nel contesto della cooperazione internazionale.
38. A tal fine, per garantire il rispetto delle norme UE, occorre inoltre promuovere la protezione dei dati in cooperazione con i paesi terzi e le organizzazioni internazionali, peraltro in linea con l'intenzione della Commissione di promuovere lo sviluppo di elevate norme di protezione dei dati, sia tecniche che giuridiche, nei paesi terzi e a livello internazionale, e di rafforzare la cooperazione con i paesi terzi<sup>(5)</sup>.

<sup>(1)</sup> Sentenza del 30 settembre 2010 nella causa T-85/09 *Kadi/Commissione*, cfr. in particolare i paragrafi 157, 177.

<sup>(2)</sup> L'allegato II (Elenco indicativo delle iniziative allo studio) del programma di lavoro della Commissione per il 2011 [COM(2010) 623 del 27 ottobre 2010] cita un «Regolamento che stabilisce la procedura di congelamento dei capitali di persone indagate per attività terroristiche nell'UE».

<sup>(3)</sup> Comunicazione della Commissione (2010) 609 del 4 novembre 2010.

<sup>(4)</sup> Cfr. la comunicazione della Commissione (2010) 573 del 19 ottobre 2010 sulla strategia per un'attuazione effettiva della Carta dei diritti fondamentali dell'Unione europea.

<sup>(5)</sup> Cfr. la comunicazione della Commissione (2010) 609 su «Un approccio globale alla protezione dei dati personali nell'Unione europea», pagg. 16-17.

39. Una chiara opportunità per promuovere l'intervento dell'Unione europea in questo settore è costituita dalle misure restrittive (congelamento dei beni), nel cui ambito l'intensa cooperazione con i paesi terzi e le Nazioni Unite non deve ridurre l'elevato livello di protezione dei diritti fondamentali garantito dal sistema giuridico dell'Unione europea.

### III. CONCLUSIONI

40. Il GEPD accoglie con favore l'attenzione riservata dalla comunicazione ai diritti fondamentali e alla protezione dei dati e raccomanda di apportare altri miglioramenti concreti nel settore della politica antiterrorismo.

41. Il GEPD raccomanda di sostenere con iniziative concrete il rispetto dei diritti fondamentali in questo settore, e in particolare il diritto alla protezione dei dati personali, che è un alleato indispensabile per promuovere la certezza del diritto, la fiducia e la cooperazione nella lotta contro il terrorismo nonché una condizione giuridica necessaria per lo sviluppo dei sistemi previsti.

42. Il GEPD sostiene altresì l'approccio secondo cui l'elaborazione di una politica sistematica in questo settore sia da preferire a una politica contingente, specialmente nel caso in cui eventuali azioni terroristiche portino alla creazione di nuovi sistemi di conservazione, raccolta e scambio dei dati senza un esame adeguato delle alternative esistenti.

43. In quest'ottica, il GEPD raccomanda alle istituzioni dell'UE di fare in modo che le politiche e le iniziative adottate nel settore degli affari interni e della sicurezza interna siano concepite e attuate in maniera tale da assicurare un approccio coerente e relazioni chiare tra loro, prevedendo sinergie adeguate e positive ed evitando duplicazioni del lavoro e degli sforzi.

44. In tale contesto, il GEPD raccomanda al legislatore UE di accrescere il ruolo della protezione dei dati impegnandosi in merito ad azioni (e scadenze) specifiche quali:

- valutare l'efficacia delle misure esistenti tenendo al tempo stesso in considerazione il loro impatto sulla vita privata è fondamentale e deve rivestire un ruolo determinante nell'azione dell'Unione europea in questo settore,

- nel prevedere nuove misure, considerare eventuali sovrapposizioni con strumenti già esistenti, tenendo conto della loro efficacia e limitando la raccolta e lo scambio di dati personali a quanto effettivamente necessario agli scopi perseguiti,

- proporre la definizione di un quadro per la protezione dei dati applicabile anche alla politica estera e di sicurezza comune,

- proporre un approccio completo e globale volto a garantire, nel settore delle misure restrittive (congelamento dei beni), sia l'efficacia dell'azione di contrasto che il rispetto dei diritti fondamentali sulla base dell'articolo 75 del TFUE,

- collocare la protezione dei dati al centro del dibattito sulle misure che disciplinano questo settore, garantendo ad esempio lo svolgimento di valutazioni di impatto sulla tutela della vita privata e sulla protezione dei dati e la consultazione tempestiva delle competenti autorità di protezione dei dati in occasione della presentazione di proposte pertinenti nel settore,

- garantire che le competenze in materia di protezione dei dati siano inserite fin dall'inizio nelle attività di ricerca sulla sicurezza in modo tale da orientare le opzioni politiche e garantire la massima integrazione possibile della vita privata nelle nuove tecnologie orientate alla sicurezza,

- assicurare l'esistenza di garanzie adeguate per il trattamento dei dati personali nell'ambito della cooperazione internazionale, promuovendo al contempo lo sviluppo e l'attuazione di principi di protezione dei dati da parte dei paesi terzi e delle organizzazioni internazionali.

Fatto a Bruxelles, addì 24 novembre 2010.

Peter HUSTINX

Garante europeo della protezione dei dati