PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3714 di martedì 09 febbraio 2016

Sul regolamento europeo per la protezione dei dati

Un'importante aggiornamento del nuovo regolamento generale europeo sulla protezione dei dati. Di Adalberto Biasiotti.

Questo documento, la cui elaborazione è stata avviata all'inizio del 2012, ha attraversato un periodo di gestazione particolarmente complesso ma è finalmente giunto all'edizione finale, che verrà ufficialmente pubblicata nella Gazzetta Ufficiale della Unione Europea presumibilmente tra marzo e aprile.
Ho presentato in precedenza una sintesi del nuovo regolamento europeo, nella versione distribuita dalla coordinatore della commissione LIBE, in data 22 ottobre 2015. Successivamente quella versione è stata aggiornata ed oggi è disponibile una versione, in data 15 dicembre 2015, che se non è proprio quella definitiva, perlomeno ci si avvicina molto.
In particolare, questo documento potrà essere soggetto a limitate revisioni, dopo che sarà stato esaminato dagli uffici legali della commissione.
Prego pertanto tutti i lettori di tenere come memoria storica il precedente documento illustrativo e, allo stato attuale, fare riferimento alla sintetica illustrazione che segue.

Il capitolo primo-indicazioni generali dà indicazioni generali sulle finalità del regolamento, gli obiettivi, l'ambito territoriale e, aspetto molto importante, offre tutta una serie di definizioni, che in questa edizione del regolamento è stata arricchita, che speriamo vengano tradotte in italiano in modo comprensibile, evitando alcune clamorose confusioni, che erano presenti nella precedente traduzione.
Mi auguro caldamente che il nostro Garante possa influenzare i traduttori europei, in modo da evitare che un responsabile del trattamento diventi un incaricato! Al proposito, faccio presente che ho inviato un messaggio personale al supervisore europeo, Giovanni Buttarelli, pregandolo di intervenire presso il comitato incaricato della traduzione.
In questo capitolo è di particolare interesse l'articolo 2, che indica con chiarezza quali sono le attività di trattamento dei dati che non rientrano nell'ambito di questo regolamento. In particolare, tutti i trattamenti aventi finalità personali, sviluppate da una persona fisica, non rientrano nell'ambito del regolamento. Parimenti, non rientrano nell'ambito di questo regolamento i trattamenti effettuati per ragione di giustizia, cui si applica una nuova direttiva, che dovrà essere approvata contemporaneamente al regolamento, entro il mese di marzo- aprile (così dicono!).

Il secondo capitolo-principi è dedicato alla illustrazione di principi generali di trattamento, che in linea di massima non sono molto diversi da quanto già era stato precedentemente definito. In particolare, il trattamento deve garantire il rispetto delle leggi in vigore, deve essere ragionevole e deve essere trasparente, nei confronti dell'interessato coinvolto.
Nell'articolo 6 vengono anche stabilite le condizioni che permettono di sviluppare il trattamento, che possono essere basate sul fatto che l'interessato abbia dato il suo consenso, che il trattamento sia necessario per l'esecuzione di un contratto o per il rispetto di obblighi legali, oppure sia indispensabile per salvaguardare la vita dell'interessato o altra persona fisica coinvolta.
Al comma 3 è messo in particolare evidenza il fatto che, ove il trattamento sia effettuato per finalità diverse da quelle per le quali i dati vennero inizialmente trattati, occorre rispettare alcune regole fondamentali, proprio per evitare che un dato possa poi essere trattato in maniera incontrollata.
L'articolo 7 fa riferimento alle modalità con cui un interessato può esprimere un valido consenso, e nell'articolo 8 vengono inserite alcune indicazioni particolari sul trattamento di dati di minori, cioè soggetti che hanno meno di 13 anni, e vengono date indicazioni in merito al trattamento di dati che vengono classificati con l'espressione "pseudo anonimi". A questo proposito, il regolamento consente che in qualche paese europeo la età minima di protezione dell'interessato possa salire a 16 anni, per facilitare l'accesso dei giovani ai "servizi della società dell'informazione".

Nell'articolo 10 viene chiarito un concetto, già presente nella nostra legislazione, che il trattamento afferente a dati che non richiedono identificazione è soggetto a regole semplificate.

Molto più interessante è **il terzo capitolo-diritti dell'interessato**, dove vengono illustrati in dettaglio i diritti degli interessati. Questo capitolo è stato ampliato in modo significativo, anche rispetto al nostro decreto legislativo 196/2003, perché nelle cinque sezioni, in cui esso è articolato, vengono presi in esame in grande dettaglio tutti gli aspetti di questi diritti.
Parliamo ora della **prima sezione-trasparenza e modalità**, che fà riferimento all'offerta di informativa. L'ultima versione del regolamento ha eliminato la prescrizione innovativa, afferente all'utilizzo di una informativa iconica, che deve essere uguale in tutta l'unione europea e che tende a superare i problemi posti dalle troppe lingue europee, nelle quali la informativa viene offerta, girando per vari paesi. Per dir la verità, non sempre questa informativa iconica è di immediata comprensione, ma dopo poco sono convinto che tutti gli interessati, vale a dire 300.000.000 di europei, potranno capirla facilmente. In particolare, il nuovo regolamento delega alla commissione europea l'incarico di stabilire forme armonizzate di offerta di informativa. Ciò non toglie che il documento elaborato dalla commissione LIBE, ed in particolare da Jean Philip Albrecht, sia comunque un interessante documento di studio, cui probabilmente la commissione potrà fare riferimento.
Nella **seconda sezione-informazioni ad accesso ai dati**, viene illustrato in dettaglio il modo in cui viene offerta la informativa (articolo 14) ed è reso possibile l'esercizio del diritto di accesso (articolo 15). Ampio spazio viene dato al diritto di rettifica e cancellazione, anche alla luce delle recenti sentenze della corte di giustizia europea, che ha ampliato in maniera significativa i diritti alla cancellazione, che sono riconosciuti all'interessato.
Nella **terza sezione-rettifica e cancellazione**, viene ampiamente illustrato il diritto all'obiezione, oppure alla limitazione dei trattamenti. Infine, nell'articolo 18 viene consolidato il diritto alla portabilità dei dati, che il data controller deve obbligatoriamente fornire all'interessato, in caso di richiesta, in un formato intellegibile e facilmente trasportabile.
La **sezione 4-diritto all'obiezione e alla assunzione di decisioni automatiche che riguardino un interessato**, fa riferimento alle modalità con cui, se consentita, è possibile sviluppare la profilazione. Sappiamo tutti che oggi i grandi motori di ricerca adottano tecniche di profilazione sempre più sofisticate, in modo da individuare e colpire il bersaglio di un eventuale messaggio pubblicitario. Ancora una volta, vengono messe in evidenza alcune limitazioni ai diritti degli interessati, che non possono evidentemente opporsi a trattamenti legati all'applicazione di tasse, indagini criminali e via di seguito
Infine, la **sezione 5-limitazioni**, mette in evidenza che leggi dell'unione europea o dei paesi membri possono porre delle limitazioni alle modalità di trattamento dei dati da parte dei data controller o data processor, in modo da rispettare i diritti fondamentali e le libertà di una società democratica.
L'articolo 21 illustra tutti i trattamenti, che potrebbero essere soggetti a queste limitazioni.
Resta inteso che esse dovranno essere sostenute da appropriate disposizioni legislative.

Il quarto capitolo-data controller e data processor è oltremodo importante perché individua i soggetti che sono preposti al trattamento dei dati. Il data controller equivale al nostro titolare ed il data processor equivale al responsabile del trattamento di dati personali, se almeno verranno rispettati i suggerimenti offerti alla commissione incaricata di curare la traduzione in italiano del regolamento.
Nella **prima sezione-obblighi generali,** ed in particolare nell'articolo 22 vengono chiaramente individuate le responsabilità del controller, che prevedono evidentemente il rispetto di tutte le leggi in vigore, ma anche di codici di condotta o schemi di certificazione, che verranno illustrati in seguito.
Questo capitolo è particolarmente importante perché comincia a mettere in evidenza alcuni strumenti, che occorre utilizzare, prima durante e dopo l'avvio di un processo di trattamento di dati personali. Questi strumenti sono illustrati nell'articolo 23. Il primo strumento viene chiamato **data protection by design**, il secondo viene chiamato **data protection by default**. Sono preziosi strumenti di analisi del trattamento, che vengono integrati successivamente da altri strumenti. Ancora una volta, viene messo in evidenza il fatto che la adozione di meccanismi di certificazione approvati può rappresentare un elemento probatorio di conformità alle indicazioni del regolamento, in fase di valutazione della legittimità e trasparenza del trattamento.
Viene anche meglio evidenziata la figura del contitolare (articolo 24), che in Italia era stato introdotto un poco tardivamente. L'articolo illustra con chiarezza come devono essere separate le responsabilità attribuite ai contitolari.
All'articolo 25 si precisa un fatto, ormai già consolidato, circa la individuazione di rappresentanti, residenti nell'unione europea, se i data controller del trattamento si trovano all'esterno dell'unione. All'articolo 26 vengono illustrate in dettaglio le mansioni del data processor, che assomiglia alquanto al responsabile del trattamento del nostro attuale decreto legislativo 196/2003. L'illustrazione è estremamente analitica e dimostra il ruolo fondamentale che svolge il data processor nel contesto di un corretto trattamento di dati personali.
Un fatto oltremodo sorprendente è legato alla scomparsa dell'incaricato del trattamento di dati personali, secondo la formulazione italiana, che perde questo nome e non ne assume alcun altro! Ovviamente esisteranno decine di migliaia di persone fisiche che tratteranno dati personali, su indicazione di data controller e data processor, ma questi soggetti sono senza nome ed ecco perché io li ho battezzati **data handler ex articolo 27**, che è l'unico punto nel quale si fà riferimento a questi

soggetti. Un'altra possibile traduzione è *addetti al trattamento di dati personali*. Vedremo cosa deciderà la commissione incaricata della traduzione.
All'articolo 28, vengono illustrate le modalità con cui devono essere documentate le modalità di trattamento e la piena disponibilità a cooperare con il garante nazionale.
La **seconda sezione-sicurezza dei dati** è tutta dedicata alla sicurezza dei dati, che richiede la introduzione di misure, proporzionate ai rischi. Dopo aver dedicato l'intero articolo 30 alle modalità che possono assicurare un elevato livello di sicurezza del trattamento, sì dà ampio spazio al **data breach**, ossia alla violazione dei dati, con indicazioni di quando e come bisogna informare il garante coinvolto ed eventuali interessati, anch'essi coinvolti.
Tutta la **terza sezione-valutazione di impatto sulla protezione dei dati e consultazione preventiva** è dedicata alla illustrazione di come devono essere protetti i dati per l'intero loro ciclo di vita. Nell'articolo 33 viene illustrato un nuovo strumento di valutazione e protezione, vale a dire il **data protection impact assessment**. Questo strumento deve essere utilizzato ogni volta che ci si trova davanti ad un trattamento che presenta rischi particolari o che comunque è incluso in una pubblica lista di attività, per le quali tali valutazioni è obbligatoria. L'autorità garante nazionale pubblica questo elenco e deve comunicarlo anche al consiglio europeo per la protezione dei dati. Parimenti, è anche possibile rendere pubblico un elenco di attività per le quali tale misura di valutazione di rischio non è richiesta.
Si passa infine, nell'articolo 34, ad illustrare i casi in cui è richiesta una **consultazione preventiva** con il garante, prima di avviare o addirittura impostare un trattamento di dati che potrebbero avere aspetti critici.
Nella **quarta sezione-data protection officer** viene illustrato un nuovo personaggio, mai conosciuto in precedenza, il data protection officer. Questo soggetto merita estrema attenzione perché la sua designazione è obbligatoria

- per tutti gli enti pubblici, con eccezione dei tribunali,
- per titolari le cui attività di trattamento richiedano il monitoraggio sistematico degli interessati, su larga scala,
- per titolari le cui attività di trattamento facciano riferimento a speciali categorie di dati, come quelle illustrate nell'articolo 9, nonché dati afferenti alla posizione giudiziaria dell'interessato, illustrate all'articolo 9 a.

È bene ricordare ai lettori che questo personaggio esiste già da molti anni nell'ambito delle istituzioni europee e quindi avremo molto da imparare dall'esperienza già maturata, per trasferirla in un contesto nazionale.
Si tratta di un soggetto che evidentemente può dare molto fastidio all'interno di un'azienda ed ecco la ragione per la quale il regolamento si preoccupa di proteggerlo in tutti i modi possibili, vedi articolo 36, ad esempio garantendo una durata minima del contratto, nonché l'attribuzione di risorse adeguate per svolgere la propria funzione. Si tratta di un professionista di elevato livello, che conosce a fondo i problemi tecnici e legali, legati al trattamento di dati personali, e che opera in piena autonomia, con la possibilità di "fare la spia" all'autorità garante, se le sue indicazioni non vengono rispettate dal data controller o data processor.
La **quinta sezione-codice di condotta e certificazione** è dedicata alla illustrazione di **codici di condotta**, di cui in Italia abbiamo già avuto una buona esperienza, ad esempio con il codice di comportamento per i giornalisti o per le ricerche storiche. In particolare, all'articolo 38a si indicano le modalità con le quali il garante nazionale può controllare e approvare i codici di condotta, sviluppati da particolari categorie di titolari o associazioni di categoria.
Per evitare di sovraccaricare le autorità garanti nazionali, è possibile monitorare la conformità a un codice di condotta, delegando a un soggetto terzo queste operazioni. In questo articolo vengono illustrate minuziosamente le modalità con cui questo potere può essere delegato ed i requisiti del soggetto terzo coinvolto. Da notare che questo tipo di monitoraggio non è consentito nei confronti di trattamenti sviluppati da autorità pubbliche.
Mi piace ricordare che questo schema non è dissimile da quello che attualmente ha adottato il ministero dell'interno, per verificare la qualità delle prestazioni che vengono offerte dagli istituti di vigilanza privata. Il ministero ha riconosciuto un certo numero di enti di certificazione terzi, accettando le valutazioni che essi rilasciano.
L'articolo 39 è dedicato ad un tema di estremo interesse, che riguarda la possibilità di introdurre meccanismi di certificazione della protezione dei dati, associati anche a sigilli sulla protezione dei dati ed altri marchi, che possono dimostrare la congruità di un trattamento con le indicazioni del regolamento. Un requisito fondamentale è che la certificazione sia volontaria e conseguibile attraverso un processo trasparente. Resta inteso che l'ottenimento di una certificazione non riduce la responsabilità del data controller o processor, ma certamente rappresenta un significativo alleggerimento.
È compito del consiglio europeo per la protezione dei dati raccogliere tutti i meccanismi di certificazione, sigilli e marchi, pubblicandoli in un registro accessibile a tutti.
L'articolo 39a fa riferimento alla struttura di questo ente di certificazione e la procedura che deve essere adottata per conseguire l'appropriato accreditamento da parte dell'autorità nazionale. I criteri di accreditamento devono essere validati dal consiglio europeo sulla protezione dei dati.
Anche la commissione europea ha titolo a "mettere becco" in questo processo.

Il capitolo quinto-trasferimento dei dati personali a paesi terzi o organizzazioni internazionali è interamente destinato alle modalità con cui è possibile trasferire dati in paesi terzi e le modalità con cui organismi internazionali, come ad esempio l'Unesco, potrebbero trattare dati personali.
Credo sia superfluo ricordare ai lettori i problemi che sono nati quando la corte di giustizia europea ha dichiarato che l'accordo **Safe harbor**, che consentiva appunto questo trasferimento tra Europa e Stati Uniti, non era soddisfacente. Ricordo anche lettori che nei primi giorni di febbraio è stata approvata una nuova bozza di accordo, che ha assunto il nome di **EU-USA privacy shield**. È troppo presto per sviluppare una valutazione approfondita di questo documento, ancora in fase di elaborazione.
All'articolo 41 si conferma, come già avviene oggi, il fatto che la commissione europea possa riconoscere un certo numero di paesi, la cui legislazione in tema di protezione dati personali sia accettabile, verso i quali quindi il trasferimento è libero. Oggi ciò vale ad esempio per Hong Kong, Nuova Zelanda e altri. Naturalmente, la commissione europea ha anche il potere di revocare questo riconoscimento.
All'articolo 42 vengono illustrate altre modalità, grazie alle quali è possibile trasferire dati in paesi terzi.
Il trasferimento è consentito in presenza di appropriate salvaguardie, debitamente esaminate e autorizzate dall'autorità garante nazionale.
Le appropriate salvaguardie sono numerose, come ad esempio la stipula di un codice di condotta approvata o la introduzione di un meccanismo di certificazione, anch'esso approvato. Tra di esse comunque quella più frequentemente adottata viene illustrata in seguito, all'articolo 43. Stiamo parlando delle famose **binding corporate rules**, che sono una sorta di protocollo di sicurezza, che deve governare lo scambio di dati tra paesi europei e altre nazioni. Nuovo ed importante l'articolo 43a, che impedisce ad un potere giudiziario o amministrativo, residente in un paese terzo, di imporre a un data processor o data controller, residente nell'unione europea, di trasferire o svelare dati personali. Sarà poi da vedere come questo articolo verrà in pratica rispettato.
All'articolo 44 vengono illustrate alcune deroghe a queste limitazioni generali, mentre l'articolo 45 auspica lo sviluppo di una cooperazione internazionale per la protezione dei dati personali.

Tutto il capitolo sesto-autorità indipendenti di supervisione (il nostro Garante) è dedicato alla illustrazione del ruolo e delle funzioni delle autorità nazionali di supervisione, come ad esempio il nostro garante.
La **sezione 1-condizioni di indipendenza** illustra il fatto che queste autorità devono essere indipendenti, imparziali, dotate di adeguate risorse e vengono date in indicazioni su come scegliere i componenti di queste autorità.
La **sezione seconda-competenze, compiti e poteri** illustra i doveri e i compiti delle autorità che, in linea di massima, non sono molto diversi da quelli attualmente in vigore, salvo la nuova possibilità di certificare i trattamenti presentati dai data controller o data processor. Ricordo che tra i compiti, chiaramente illustrati all'articolo 52, vi è l'obbligo di

- garantire l'applicazione del regolamento,
- sensibilizzare il pubblico sui problemi legati al trattamenti non appropriati,
- offrire indicazioni al governo e al Parlamento, quando vengono elaborati leggi afferenti al trattamento di dati personali,
- indagare su possibili violazioni sul regolamento e
- accettare reclami presentati da un interessato.

È esplicitamente imposto il vincolo che la gestione dei reclami degli interessati debba essere fatta gratuitamente, salvo casi affatto particolari. Non elenco tutti i compiti in forma analitica, ma basta dare un'occhiata al testo per rendersi conto che certamente l'autorità garante nazionale avrà parecchio da fare!

Il settimo capitolo- cooperazione e coerenza è assai articolato.
La **sezione 1-cooperazione** è interamente dedicata alla illustrazione di come le autorità garanti nazionali possono collaborare con altre autorità garanti. L'articolo 55 mette chiaramente in evidenza un obbligo di mutua assistenza, anche quando una nazione non ha designato una sola autorità garante nazionale, ma più autorità garanti. In questo caso una sola deve interfacciarsi con i garanti di altri paesi.
La **sezione 2-congruità** mira a far sì che le attività svolte dai singoli paesi, in particolare le singole autorità garanti, non portino a sviluppare percorsi differenziati e perfino in contrasto tra loro, come purtroppo è avvenuto quando è entrata in vigore la direttiva europea sulla protezione dei dati personali e tale direttiva è stata recepita in ogni paese con leggi spesso assai diverse fra di loro.
L'opera di vigilanza sull'attività di questi garanti, che hanno un certo margine di discrezionalità, anche se normalmente inferiore rispetto a quello oggi in vigore, è affidata allo**European data protection board**, il quale anche il compito di risolvere eventuali conflitti tra le autorità garanti nazionali (articolo 58a). L'articolo 61 è dedicato all'illustrazione delle modalità con cui è possibile invocare una procedura d'urgenza, afferente ad attività critiche o conflittuali di trattamento di dati personali.
Il capitolo si conclude con la **sezione 3-consiglio europeo per la protezione dei dati** che illustra il ruolo e le funzioni

dell'European data protection board, di cui fa parte il rappresentante di ogni autorità garante e lo **European the data protection supervisor** (oggi è Giovanni Buttarelli). I compiti affidati a questo consiglio sono numerosi e sono puntualmente elencati nell'articolo 66. In pratica, si tratta di un organo di sorveglianza, armonizzazione e monitoraggio, che ha il potere-dovere di emettere pareri su un gran numero di attività. È evidente l'obiettivo del legislatore, che vuole evitare, ancora una volta, possibili fughe in avanti o di lato delle varie autorità garanti nazionali.
Ad ogni buon fine, all'articolo 67 si impone che questo consiglio pubblichi annualmente un rapporto sull'attività svolta.
Ampio spazio infine è dedicato alla illustrazione del ruolo del supervisore di questo consiglio, che, insieme al segretario, deve garantire l'armonioso funzionamento della struttura.

Il capitolo otto-rimedi, responsabilità e sanzioni è dedicato alla illustrazione delle differenze fra il procedimento di tutela amministrativa e quello di tutela giudiziaria, come già avviene oggi in Italia. Parimenti, è sempre riconosciuto il diritto di ricorrere alla tutela giudiziaria, in caso di insoddisfazione con i provvedimenti emessi dagli organi di tutela amministrativa.
Parimenti interessante è l'articolo 76, che riconosce alle associazioni di categoria il potere di rappresentare interessati, aventi caratteristiche omogenee o problematiche similari. Si tratta di una sorta di class action, che viene riconosciuta del regolamento.
L'articolo 77 mette in evidenza l'esistenza di una responsabilità solidale del data controller e data processor, che sono quindi intimamente coinvolti nel trattamento dei dati, salvo diverse pattuizioni contrattuali, che dovrebbero essere ben evidenziate.
L'articolo 79 illustra le condizioni generali per imporre delle sanzioni amministrative, senza però entrare in valutazioni analitiche. Vengono date delle indicazioni generali, lasciando liberi i vari paesi di stabilire sanzioni amministrative efficaci, proporzionate e dissuasive, che non è detto siano esclusivamente economiche. Solo per alcuni particolari violazioni sono indicate specifiche categorie di sanzioni, in particolare al comma 3, che indica in sanzioni amministrative fino a 10.000.000 di euro o, in caso di gruppi di aziende, fino al due percento del fatturato dell'anno precedente, per violazioni degli obblighi del data controller o del data processor. Per contro, le sanzioni salgono a 20.000.000 di euro e fino al quattro percento del fatturato globale se vengono ignorati i principi fondamentali del trattamento, inclusa la raccolta del consenso e la violazione dei diritti degli interessati o il trasferimento non autorizzato di dati in un paese terzo.
Infine, anche il mancato rispetto di un provvedimento emesso da una autorità garante nazionale porta all'applicazione di sanzioni similari.
Resta inteso che contro la erogazione di queste sanzioni è sempre consentito il ricorso alla tutela giudiziaria.
Per quanto riguarda le responsabilità penali, si legga l'articolo 79d, che ha delegato ai singoli paesi la emissione di provvedimenti legislativi specifici. Ai lettori che ritengono che queste sanzioni possano essere troppo elevate, raccomando di vedere cosa accade in Italia, laddove i gestori telefonici, che ripetutamente vengono sanzionati dal garante, non cambiano per niente i loro comportamenti. Si vede che certi comportamenti portano profitti assai più alti di quanto non sia la sanzione relativa.

Il capitolo 9-provvedimenti legati a specifiche situazioni di trattamento dei dati offre alcune disposizioni afferenti a specifiche attività di trattamento e illustra in particolare alcune peculiarità del trattamento applicabili ai numeri identificativi nazionali, come ad esempio il nostro codice fiscale, ai dati personali dei dipendenti, a dati trattati per finalità scientifiche e per i servizi di archivio (articolo 83). Un articolo è dedicato specificamente ai problemi di trattamento di dati personali religiosi (articolo 85).

Il decimo capitolo-atti delegati ed attuativi illustra i decreti delegati ed attuativi da emanare; esso ricorda che è possibile elaborare dei formati standardizzati per dare attuazione alle disposizioni del regolamento e l'esempio più evidente, come accennato in precedenza è quello del formato standard di informativa. La commissione europea è delegata a elaborare questi atti, con l'assistenza di una specifica commissione specializzata.

Il capitolo undicesimo-provvedimenti finali fà riferimento alle disposizioni finali e indica i precedenti testi legislativi o direttive che vengono superati da questo regolamento. Inoltre si impone alla commissione europea di riferire al Parlamento in merito alle modalità di applicazione a questo regolamento. S'intende che la commissione europea è comunque sempre legata a doppio filo con il Parlamento europeo e il consiglio dell'unione europea, nonché ad altri enti che abbiano voce in capitolo in fase di trattamento dei dati personali.
Il primo rapporto della commissione verrà emesso entro quattro anni dall'entrata in vigore di questo regolamento e dovrà essere reso pubblico. È anche facoltà della commissione presentare proposte di modifica del regolamento.
Il regolamento entra in vigore nel dodicesimo giorno seguente alla pubblicazione sul giornale ufficiale dell'unione europea.

Commento finale
Come accennato in precedenza, nella versione emessa in data 15 dicembre 2015 di questo regolamento è stato tolto l'annesso 1, afferente alla presentazione iconica dell'informativa. Ho preferito comunque inserirlo egualmente perché potrebbe essere un utile strumento di riferimento non solo per la commissione, ma anche per qualsiasi data processor che debba sviluppare una

informativa iconica, facilmente intelligibile in tutti i paesi dell'unione europea.

Annesso1 la presentazione iconica della informativa, che mi auguro tutti vorranno studiare attentamente e che potrebbe essere già applicata fin da oggi, per chi ha voglia di cavalcare la tigre.

Le nuove icone della privacy

Adalberto Biasiotti
