IL NUOVO REGOLAMENTO PRIVACY EUROPEO

CURIOSITA' IN PILLOLE SU QUELLO CHE CI ASPETTA

Avv. Luca Bolognini

Presidente dell'Istituto Italiano per la Privacy
Founding partner ICT Legal Consulting

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

Applicazione in due anni

Solo trattamenti di dati personali (esclusi i dati non personali) mentre la Direttiva 2002/58/CE prende in considerazione anche i dati comunque presenti all'interno dei dispositivi di comunicazione privati

La Direttiva e-Privacy (2002/58/CE) andrà modificata, ma continua ad applicarsi, con riferimento ai trattamenti di dati personali, laddove prevede obblighi specifici per i communication service provider

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

Finalità esclusivamente personali e domestiche

Il Regolamento non si applica a trattamenti per finalità esclusivamente personali e domestiche. Non c'è più l'eccezione, però, della comunicazione sistematica e della diffusione (problema: come inquadrare gli utenti generanti contenuti pubblici on line?)

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

GLI ISSP FINALMENTE NON RESPONSABILI

Il regolamento lascia impregiudicata l’applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui ai suoi articoli da 12 a 15.

Ottimo. Ma un responsabile di un'illecita diffusione di dati su un social network dovrà pur esserci (l'utente?)

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

LEX DOMICILII PER I DATI

Il regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti residenti nell'Unione,

b) il controllo del loro comportamento.

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

L'INTERESSATO, MA CON RAGIONEVOLEZZA

“Interessato”: la persona fisica identificata o identificabile, direttamente o indirettamente, con mezzi che il responsabile del trattamento o altra persona fisica o giuridica **ragionevolmente** può utilizzare, con particolare riferimento a un numero di identificazione, a dati relativi all’ubicazione, a un identificativo on line o a uno o più elementi caratteristici della sua identità genetica, fisica, fisiologica, psichica, economica, culturale o sociale.

Se i dati trattati da un responsabile del trattamento non consentono di identificare una persona fisica, il responsabile del trattamento non è obbligato ad acquisire ulteriori informazioni per identificare l’interessato al solo fine di rispettare una disposizione del regolamento.

CONSENSO ESPLICITO E INEQUIVOCABILE

“Consenso dell’interessato”: qualsiasi manifestazione di volontà libera, specifica, informata ed esplicita con la quale l’interessato accetta, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

IMPRESE FISICHE?

“Impresa”: ogni entità, indipendentemente dalla forma giuridica rivestita, che eserciti un’attività economica, comprendente pertanto, in particolare, le persone fisiche e giuridiche, le società di persone o le associazioni che esercitano un’attività economica

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

C'E' LA CRISI: L'EQUITA' SOSTITUISCE LA CORRETTEZZA

- In realtà, la parola inglese è sempre “fairly”, che questa volta, però, viene tradotto come modo “equo”

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

Nuovo principio: ACCOUNTABILITY

I dati sono trattati sotto la responsabilità del responsabile del trattamento, che assicura e comprova, per ciascuna operazione, la conformità alle disposizioni del regolamento.

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

IL LEGITTIMO INTERESSE DEL TITOLARE RENDE LECITO IL TRATTAMENTO

Il trattamento è lecito se necessario per il perseguimento del legittimo interesse del responsabile del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Incombe sul responsabile del trattamento dimostrare che i suoi legittimi interessi possono prevalere sull'interesse o sui diritti e sulle libertà fondamentali dell'interessato.

Direct marketing cartaceo in opt-out?

CONSENSO PRIVACY: APPROCCIO “VESSATORIO”

Se il consenso dell’interessato deve essere fornito nel contesto di una dichiarazione scritta che riguarda anche altre materie, l’obbligo di prestare il consenso deve essere presentato in forma distinguibile dalle altre materie.

Il consenso non costituisce una base giuridica per il trattamento ove vi sia un notevole squilibrio tra la posizione dell’interessato e del responsabile del trattamento. Sempre revocabile.

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

Sweet Thirteen: bambini più tutelati

Per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali di minori di età inferiore ai tredici anni è lecito se e nella misura in cui il consenso è espresso o autorizzato dal genitore o dal tutore del minore. Il responsabile del trattamento si adopera in ogni modo ragionevole per ottenere un consenso verificabile, in considerazione delle tecnologie disponibili.

Come si fa? Ce lo dirà la Commissione Europea

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

I NUOVI DATI SENSIBILI

Sono i dati personali che rivelino la razza, l'origine etnica, le opinioni politiche, la religione o le convinzioni personali, l'appartenenza sindacale, come pure trattare dati genetici o dati relativi alla salute e alla vita sessuale o a condanne penali o a connesse misure di sicurezza.

Attenzione: diventa lecito trattarli se "il trattamento riguarda dati resi manifestamente pubblici dall'interessato"

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

TRATTAMENTI DI DATI SULLA SALUTE PER PRESTAZIONI SANITARIE DI DIAGNOSI E CURA

Non servirà più il consenso dell'interessato, se trattati da personale sanitario tenuto al rispetto del segreto professionale

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

INFORMATIVE A FUMETTI

Il responsabile del trattamento fornisce all’interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in forma intelligibile, con linguaggio semplice e chiaro e adeguato all’interessato, in particolare se le informazioni sono destinate ai minori.

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

RISCONTRO AL DIRITTO D'ACCESSO

Si passa dai vecchi 15 giorni (+ 15) a 30 giorni + 30 se più interessati esercitano i loro diritti e la loro cooperazione è necessaria in misura ragionevole per evitare un impiego di risorse inutile e sproporzionato al responsabile del trattamento

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

INFORMATIVA (DI POLIZIA?)

Nell'informativa dovremo indicare anche il diritto di proporre reclamo all’autorità di controllo e le coordinate di contatto di detta autorità

Clausola-voragine: dovremo anche fornire ogni altra informazione necessaria per garantire un trattamento equo nei confronti dell’interessato, in considerazione delle specifiche circostanze in cui i dati personali vengono raccolti.

Diritto all'oblio: i dati vanno tenuti al guinzaglio

L’interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un’ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l’interessato era un Minore (under-18). Quando ha reso pubblici dati personali, il responsabile del trattamento prende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell’interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione.

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

Diritto alla portabilità del dato

L’interessato ha il diritto, ove i dati personali siano trattati con mezzi elettronici e in un formato strutturato e di uso comune, di ottenere dal responsabile del trattamento copia dei dati trattati in un formato elettronico e strutturato che sia di uso comune e gli consenta di farne ulteriore uso.

Attenzione: la portabilità è diritto degli interessati, non di un titolare/responsabile rispetto ai dati personali di terzi collocati su un sistema altrui (es. cloud)

Protezione dalla profilazione

Chiunque ha il diritto di non essere sottoposto a una misura che produca effetti giuridici o significativamente incida sulla sua persona, basata unicamente su un trattamento automatizzato destinato a valutare taluni aspetti della sua personalità o ad analizzarne o prevederne in particolare il rendimento professionale, la situazione economica, l’ubicazione, lo stato di salute, le preferenze personali, l’affidabilità o il Comportamento.

Se i dati sono trattati in base a contratto o con il consenso dell'interessato, o nel rispetto di una disposizione di legge, devono essere chiaramente previste e indicate le garanzie a tutela dei suoi legittimi interessi (anche nella legge).

Il trattamento automatizzato di dati personali destinato a valutare taluni aspetti della personalità dell’interessato non può basarsi unicamente sulle categorie particolari di dati personali sensibili.

Abbiamo scherzato? Gli Stati possono superare principi e regole privacy

L'Unione o gli Stati membri possono limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui all'articolo 5, lettere da a) a e), agli articoli da 11 a 20 e all'articolo 32, qualora tale limitazione costituisca una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la pubblica sicurezza; b) le attività volte a prevenire, indagare, accertare e perseguire reati; c) altri interessi pubblici dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, e la stabilità e l'integrità del mercato; d) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; e) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere a), b), c), e d); f) la tutela dell'interessato o dei diritti e delle libertà altrui.

Corresponsabili (joint controllers)

Se il responsabile del trattamento determina le finalità, le condizioni e i mezzi del trattamento dei dati personali insieme ad altri, i corresponsabili del trattamento determinano, mediante accordi interni, le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal regolamento, con particolare riguardo alle procedure e ai meccanismi per l’esercizio dei diritti dell’interessato.

ALTRO CHE DPS, DOVREMO DOCUMENTARE TUTTO E DI PIU'

Ogni responsabile del trattamento, incaricato del trattamento ed eventuale rappresentante del responsabile del trattamento conserva la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità.

Per i dettagli, leggetevi gli articoli 28 e 22 del Regolamento

PRIVACY IMPACT ASSESSMENT

Quando il trattamento, per la sua natura, il suo oggetto o le sue finalità, presenta rischi specifici per i diritti e le libertà degli interessati, il responsabile del trattamento o l’incaricato del trattamento che agisce per conto del responsabile del trattamento effettua una valutazione dell’impatto del trattamento previsto sulla protezione dei dati personali.

DATA PROTECTION OFFICER

Il responsabile del trattamento e l'incaricato del trattamento designano sistematicamente un responsabile della protezione dei dati quando:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico,

b) il trattamento è effettuato da un'impresa con 250 o più dipendenti,

c) le attività principali del responsabile del trattamento o dell'incaricato del trattamento consistono in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati.

Requisiti: conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati e piena indipendenza

CODICI DI CONDOTTA E CERTIFICAZIONI (BOLLINI)

Potranno essere riconosciuti, dalle autorità indipendenti o dalla Commissione, i codici di condotta di associazioni e organismi di categoria, se conformi al Regolamento, con le relative risoluzioni alternative delle controversie privacy.

Gli Stati membri e la Commissione incoraggiano, in particolare a livello europeo, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati garantito dai responsabili del trattamento e dagli incaricati del trattamento.

Le associazioni possono ricorrere alle autorità di controllo

Ogni organismo, organizzazione o associazione che tuteli i diritti e gli interessi degli interessati in relazione alla protezione dei loro dati personali e che sia debitamente costituito o costituita secondo la legislazione di uno Stato membro ha il diritto di proporre reclamo all'autorità di controllo di qualunque Stato membro per conto di uno o più interessati qualora ritenga che siano stati violati diritti derivanti dal regolamento a seguito del trattamento di dati personali.

Indipendentemente dall'eventuale reclamo dell'interessato, ogni organismo, organizzazione o associazione che ritenga che sussista violazione dei dati personali ha il diritto di proporre reclamo all'autorità di controllo di qualunque Stato membro.

Tutela giurisdizionale: foro del titolare... ma anche dell'interessato

Le azioni contro il responsabile (titolare) del trattamento o l’incaricato del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il responsabile del trattamento o l’incaricato del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l’interessato risiede abitualmente, salvo che il responsabile del trattamento sia un’autorità pubblica nell’esercizio dei pubblici poteri.

Sanzioni stellari

Fino al 2% del fatturato globale: il tema della compliance privacy europea entra, finalmente, anche nei board e nei cda dei grandi colossi multinazionali, come già è per l'antitrust

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY

Dalla sanzione al perdono: le Autorità religiose indipendenti

Qualora in uno Stato membro chiese e associazioni o comunità religiose applichino, al momento dell’entrata in vigore del presente regolamento, corpus completi di norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali, tali corpus possono continuare ad applicarsi purché siano conformi alle disposizioni del regolamento. Le chiese e le associazioni religiose che applicano i corpus completi di norme di cui sopra provvedono a istituire un’autorità di controllo indipendente ai sensi del regolamento.

Grazie

luca@lucabolognini.it

WWW.ISTITUTOITALIANOPRIVACY.IT

ICT LEGAL CONSULTING

ISTITUTO ITALIANO PRIVACY