Tutela della privacy

“Regolamento Europeo”
GENERAL DATA PROTECTION REGULATION
GDPR
Regolamento UE 2016/679


CryptoLocker
Payment for private key
bitcoin
• Choose the amount of payment:
2 BTC
• Send coins to the following address:
Attention!
Make sure that you enter the payment information correctly! Each incorrect attempt will reduce the time to destroy the private key in half!
Are you sure you entered your payment information correctly?
Yes
No
Time left
43 : 30 : 40
<< Back
PAY

Data protection laws in European Union

Dir. 95/46 – Dir. 2002/58 – Dir. 2009/12 implemented with

Austria	Data Protection Act No. 165/1999 (*DatenSchutzGesetz*)
Belgium	Data Protection Act, 8 December 1992
Bulgaria	Personal Data Protection Act, January 2002
Croatia	Personal Data Protection Law 103/2003
Cyprus	Law of 2001, November 2001
Czech Republic	Act no. 101/2000 Coll.
Denmark	Act on Processing of Personal Data, June 2000
Estonia	Data Protection Act, 1 January 2008
Finland	Personal Data Act 523, (Henkilötietolaki), June 1999
France	Law No. 2004-801, 6 August 2004 (already had *Law No. 78/17*)
Germany	Federal Data Protection Act (*BundesDatenSchutzGesetz*)
Greece	Law 2472/1997, October 1997
Hungary	Act No. CXII, 1 January 2012
Ireland	Data Protection Act 1988 amended in 2003
Italy	Law 675/1996 and Legislative Decree 196/2003
Latvia	Personal Data Protection Law, 7 March 2014)
Lithuania	Law 11 June 1996 amended in 2000 with Law 17 July 2000
Luxembourg	Law 2 August 2002
Malta	Data Protection Act (Act) (Chapter 440 of the Laws of Malta)
Netherlands	Dutch Personal Data Protection Act (Wbp), 1 September 2001
Poland	Personal Data Protection Act, 29 August 1997
Portugal	Law nº. 67/98, October 26
Romania	Law no 677/2001, November 2001
Slovakia	Act No. 428/2002 Coll., September 2002
Slovenia	Personal Data Protection Act, ZVOP, Ur.l. RS No. 59/99
Spain	Special Data Protection Act 1999, November 1999
Sweden	Personal Data Act (Sw. *personuppgiftslagen*, SFS 1998:204)
United Kingdom	Data Protection Act 1998

Reg. 679/2016 no implementation but

Reform of DSG started in May 2017

Reform of BDSG started in February 2017

This Regulation also provides a margin of manoeuvre for Member States to specify its rules (Whereas n. 10)

ART. 1 GDPR
Oggetto e finalità

- Il presente regolamento stabilisce norme relative alla protezione **delle persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

- 2.Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

- 3.La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

COSA E' CAMBIATO ?

DIRITTO ALL'OBLIO

COSA E' CAMBIATO ?

PORTABILITA' DEI DATI

COSA E' CAMBIATO ?

ABOLIZIONE DELLA NOTIFICAZIONE

COSA E' CAMBIATO ?

DATA BREACH

COSA E' CAMBIATO ?

SANZIONI PARI AL 2-4% DEL FATTURATO

Ambiti di Applicazione – Art. 3

Il Regolamento si applica a:

Imprese con almeno uno stabilimento nell'Unione

Indipendentemente dal fatto che il trattamento sia effettuato nell'UE

Imprese che non hanno uno stabilimento nell'UE, nei seguenti casi:

Offerta di beni o servizi (anche gratuiti) agli Interessati nel territorio dell'UE

Monitoraggio del comportamento degli Interessati all'interno dell'Unione

Imprese che non hanno uno stabilimento nell'UE, ma:

Con stabilimento in un luogo soggetto al diritto di uno Stato Membro

Il Regolamento trova applicazione anche nei confronti di Big Data e c.d. colossi del web (Facebook, Google, etc.)

Art. 27: Nei casi di soggetti che non hanno uno stabilimento nell'UE, il Titolare o il Responsabile designa per iscritto un Rappresentante nell'Unione. Tale obbligo non si applica ai trattamenti occasionali e alle autorità o organismi pubblici.

Il Rappresentante non è solamente un interlocutore, ma è anche soggetto ad eventuali atti di esecuzione, fatte salve le azioni legali nei confronti del Titolare o del Responsabile del trattamento.

“Nuove Definizioni e Categorie di Dati”

Soggetti Coinvolti

Codice Privacy:	Regolamento Europeo:
	
Titolare del Trattamento	Data Controller o Titolare del Trattamento
	
Responsabile Esterno del Trattamento Amministratore di Sistema	Joint Controller o Contitolare del Trattamento
	
Responsabile ed Incaricato del Trattamento	Data Processor o Responsabile del Trattamento
	
Responsabile della Sicurezza dei Dati Personali	Data Protection Officer

Titolare o Responsabile? – Capo IV

Il testo originale del Regolamento Europeo prevedeva solo la figura di Responsabile del Trattamento e dell'Incaricato.

Il 13 aprile 2016 il Garante della Privacy ha annunciato che la traduzione italiana del Regolamento avrebbe mantenuto la struttura gerarchica già presente nel Codice Privacy, andando ad introdurre nuovamente la figurare del Titolare del Trattamento.

I termini "Titolare del trattamento" e "Responsabile del trattamento", già presenti nel Codice privacy italiano, compariranno anche nei testi italiani del Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola i settori di prevenzione, contrasto e repressione dei crimini, entrambi in invia di approvazione definitiva a Bruxelles.

Si tratta di un adattamento terminologico caldeggiato dal Garante per la protezione dei dati personali preoccupato di non veder sottoposti gli operatori del nostro Paese ad un inutile sforzo adattativo e interpretativo. L'iniziativa del Garante ha trovato anche il sostegno dei giuristi-linguisti di lingua italiana presso il Consiglio e il Parlamento Ue.

Le precedenti versioni italiane del Regolamento, infatti, riportavano i termini "responsabile del trattamento" (data controller) e "incaricato del trattamento" (data processor). Tuttavia, trattandosi, di fatto, di figure identiche quanto a caratteristiche soggettive a quelle che nel Codice privacy italiano sono indicate rispettivamente come "titolare" e "responsabile", l'Autorità italiana ha chiesto ed ottenuto che i nuovi testi mantenessero tali diciture in modo da evitare a imprese, enti, professionisti e cittadini ogni possibile problema di interpretazione giuridica ed eventuali costi, anche materiali, connessi al cambiamento terminologico.

Il TITOLARE DEL TRATTAMENTO

- Il Titolare del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza.

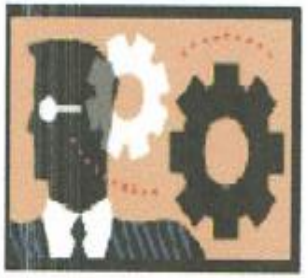
- E' onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che:

- assicurino e garantiscano che vengano adottate le misure di sicurezza previste dal GDPR e del Codice in materia di trattamento dei dati personali;

- adottino delle misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il RESPONSABILE (2/3)

"Interno"



- *Coadiuva il Titolare negli obblighi privacy*
- *Nomina opzionale*
- *"Obbligata" se organizzazione complessa*
- *Deve presentare adeguate garanzie di competenza*
- *Ha assegnato compiti scritti e riceve istruzioni*
- *Puo' designare gli incaricati*

CHI PUO' ESSERE IN AZIENDA?

PERSONA DI ALTO PROFILO / COMPETENZA

(es. Dir. Legale, Personale, Vendite, Organizzazione, Compliance Manager...)

Il RESPONSABILE (3/3)

"Esterno"

- Soggetto che tratta dati per conto del Titolare
- New Ruolo "obbligatorio" in caso di esternalizzazione di attività (es: predisposizione cedolini, gestione sistema informativo, call center, agenti...)
- Puo' essere persona fisica o giuridica
- Deve presentare adeguate garanzie di rispetto del Regolamento
- New I trattamenti esternalizzati devono essere disciplinati da un contratto (o atto giuridico) scritto, sottoscritto per accettazione
- New Il contratto deve prevedere una serie di vincoli prestabiliti (art28)

CHI E' ALL' ESTERNO DELL' AZIENDA

CIASCUN OUTSOURCER

E gli Incaricati?

Il testo del regolamento fa riferimento in più punti a *persone autorizzate al trattamento*, senza però fornire una precisa definizione o un ruolo (Art. 30 Codice Privacy: Incaricati / Data Handler).

La figura dell'Incaricato è rilevante soprattutto in ottica di Accountability, poiché potrebbe essere utile nel dimostrare l'adozione di tutte le misure tecniche ed organizzative adeguate a garantire un trattamento conforme dei dati, e nell'individuare i centri di responsabilità privacy.

Etichettare i ruoli è fondamentale poiché favorisce la rintracciabilità dei Soggetti coinvolti nel trattamento dei dati, soprattutto da parte dell'Interessato.

Il GDPR non mette in discussione l'Incaricato del Trattamento (ex art. 30 196/03). Tale articolo non è in conflitto, ma compatibile con GDPR, pertanto potrebbe rimanere in vigore. Il GDPR abroga la Direttiva 95/46, non Codice il Privacy.

Nella 27001 e nella 231 la sicurezza informatica e la correttezza del trattamento dipendono quasi esclusivamente dalla persona autorizzata al trattamento dei dati. Nell'ottica della 231, l'adeguatezza del Modello Organizzativo Privacy è fondamentale anche da un punto di vista penale, al fine di determinare i soggetti responsabili penalmente.

INCARICATI DEL TRATTAMENTO

- Tutti gli operatori che trattano dati personali devono almeno essere designati, ancora con atto scritto, quali “incaricati del trattamento”. Ogni incaricato deve attenersi alle istruzioni ricevute dal responsabile. La nomina degli Incaricati del trattamento deve essere controfirmata dall’interessato per presa visione e copia della stessa deve essere conservata a cura del Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.

- Agli Incaricati del trattamento il Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

INCARICATI DEL TRATTAMENTO

- La nomina degli Incaricati è a tempo indeterminato, e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.
- Nell'assolvimento del loro compito gli Incaricati del Trattamento dovranno osservare scrupolosamente le seguenti istruzioni:

ISTRUZIONI PER GLI INCARICATI

- Al primo accesso alle banche dati, delle quali effettueranno il trattamento, ogni incaricato provvederà a modificare la password assegnatagli e a modificarla ogni sei mesi. Nel caso venissero trattati dati sensibili o giudiziari, la password andrà modificata ogni tre mesi. Sarà cura di ogni incaricato garantire la segretezza delle proprie credenziali di autenticazione

Joint Controller – Art. 26

Si tratta del così detto Titolare Congiunto, o meglio ancora del Contitolare del Trattamento dei Dati: nello specifico, per un medesimo trattamento di dati personali, potranno sussistere due responsabili del trattamento.

Titolare del Trattamento

Joint Controller

Se più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali, essi sono Contitolari del trattamento e determinano le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal Regolamento.

I Contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi.

Il contenuto essenziale dell'accordo è messo a disposizione dell'Interessato, che può esercitare i propri diritti nei confronti di ciascun soggetto. Ma l'Autorità Garante quale soggetto andrebbe a colpire in caso di illecito?

Categorie di Dati Attuali

Dati Comuni

- Anagrafici
- Indirizzi Postali/Telematici
- Codici Indentificativi

Dati Giudiziari

- Iscrizioni casellario giudiziario in materia penale, condanna, abitualità nel reato, ecc

Dati Quasi Sensibili

- Presentano rischi per libertà/dignità
- Accorgimenti dettati dal Garante: «Prior Checking»

Dati Sensibili

- Origine raziale / etnica
- Convinzioni religiose, filosofiche, politiche
- Stato di Salute / Vita sessuale

Attuale Definizione di Dati Sensibili

Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti e sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Origine Razziale / Etnica

Opinioni Politiche

Convinzioni Religiose

Dati Medico Sanitari

Vita Sessuale

I Dati Sensibili diventano Particolari – Art. 9

Dati personali che rivelino razza, origine etnica, opinioni politiche, religione o le convinzioni personali, appartenenza sindacale, dati relativi alla salute, alla vita e orientamento sessuale, come anche dati genetici e biometrici, ~~o dati relativi a condanne penali o a connesse misure di sicurezza~~.

Origine Razziale / Etnica

Opinioni Politiche

Convinzioni Religiose

Dati Relativi alla Salute

Vita Sessuale

Dati Biometrici

Dati Genetici

~~Condanne Penali e Reati~~

Diventa lecito trattarli se il trattamento riguarda dati resi manifestamente pubblici dall'interessato.

Dati Relativi alla Salute – Art. 9

Per il trattamento di dati relativi alla salute del soggetto Interessato anche per prestazioni sanitarie, di diagnosi e cura, non servirà più il consenso dell'Interessato, se tali dati vengono trattati da personale medico-sanitario, in quanto gli stessi soggetti sono tenuti al rispetto del segreto professionale.

Dati Relativi alla Salute anche per Prestazioni di Diagnosi e Cura

Trattati da Personale tenuto al Segreto Professionale

Non Necessario il Consenso

Dati Relativi a Condanne Penali – Art. 10

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, può avvenire soltanto sotto il controllo dei pubblici poteri o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda adeguate garanzie per i diritti e le libertà degli interessati.

Condanne Penali e Reati

Sotto il Controllo dei Pubblici Poteri

Autorizzato dal diritto dell'Unione o Stati membri

Adeguate Garanzie per Diritti e Libertà degli interessati

Un registro completo delle condanne penali può essere tenuto soltanto sotto il controllo dei pubblici poteri.

“Principi introdotti dal Regolamento e modifiche apportate”

Principio di Accountability - Art. 24

~~Il responsabile del trattamento adotta politiche e attua misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme al presente regolamento.~~

Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al presente regolamento.

Campo di Applicazione, Contesto, Finalità, Rischi e Gravità per i Diritti

Misure Tecniche e Organizzative Adeguate

Onere della Prova: Dimostrare che il Trattamento è Conforme

New

ACCOUNTABILITY

Responsabilizzazione e obbligo generale di Prova degli adempimenti –art 24

- **CHI E' OBBLIGATO**
  - *IL TITOLARE*
- **COSA DEVE FARE**
  - ***OPERARE***
    - ✓ *Mettere in atto misure Tecniche e Organizzative adeguate*
    - ✓ *Anche mediante pubblicazione e attuazione di politiche adeguate*
  - ***DARE DIMOSTRAZIONE***
    - ✓ *Essere in grado di dimostrare che i trattamenti avvengono in conformità al Regolamento*
  - ***AGGIORNARE***
    - ✓ *Verificare periodicamente le misure e aggiornarle*

NOTA: *Il rispetto degli obblighi può essere dimostrato attraverso l'adesione a codici di condotta o al meccanismo di certificazione (art 40,42)*

Informativa Chiara e Semplice - Art. 13

Il Titolare del trattamento fornisce all'interessato tutte le informazioni relative al trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare le informazioni destinate specificamente ai minori.

Identità del Titolare (e DPO)

Finalità del Trattamento

Base Giuridica del Trattamento

Legittimi Interessi Perseguiti

Destinatari dei dati personali

Trasferimento dei Dati

Periodo di Conservazione dei Dati

Diritto di Accesso ai Dati

Revoca del Consenso

Diritto di Proporre Reclamo

Obbligatorietà comunicazione Dati

Processi Automatizzati (Profilazione)

Informativa - Art. 14

In caso di dati non raccolti presso l'Interessato è inoltre necessario fornire queste ulteriori informazioni:

Categorie dei Dati

Fonte da cui hanno origine i Dati

Eventuale provenienza da fonti accessibili al pubblico

Il Titolare deve fornire l'informativa al massimo entro un mese dall'ottenimento dei dati o al momento della prima comunicazione con l'Interessato o divulgazione degli stessi.

In caso di trattamento dei dati per ulteriori finalità occorre fornire una nuova informativa all'Interessato.

Casi di esclusione:

L'Interessato dispone già di tali informazioni

La comunicazione è impossibile o implica risorse sproporzionate

Trattamento previsto dal diritto degli Stati Membri e UE

Trattamento soggetto a Segreto Professionale

Consenso Inequivocabile - Art. 4

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.

Rimosso il termine "Consenso Esplicito" dal testo

Passaggio al "Consenso Inequivocabile" ovvero anche per "Fatti Concludenti"

Non configura consenso il consenso tacito o passivo o la preselezione di caselle

Se il consenso è richiesto con modalità elettronica, la richiesta deve essere chiara, concisa e non disturbare inutilmente il servizio per il quale il consenso è espresso.

IL CONSENSO (1/4)

Condizione di LICEITA'

COS'E'

- *E' la condizione necessaria per poter trattare i dati in modo lecito, in assenza di una delle altre condizioni previste dalla legge (es. esecuzione contratto, obbligo di legge...)*
- *Deve essere richiesto in chiusura dell'Informativa*
- *Risposta dell'interessato all' Informativa*

SCOPO

- *Autorizzare o negare l'uso dei dati*

CONDIZIONI DI VALIDITA'

- ***INFORMATO** invalido se non preceduto da informativa*
- ***SPECIFICO,** richiesto in modo chiaro e distinguibile dal resto*
- New ***LIBERO** svincolato da costrizioni . es. l'esecuzione del contratto non deve essere subordinata al rilascio del Consenso per l' invio di pubblicità*
- New ***CONSAPEVOLE E INEQUIVOCABILE,** basato su dichiarazione o azione positiva- No caselle pre-barrate*

IL CONSENSO (2/4)

- **LA PLURALITA' DEI CONSENSI**
  - ***Diritto di esprimere Consenso per una o più finalità***
  - ***Esempi di finalità aggiuntive:***
    - ✓ *Profilazione,*
    - ✓ *Invio di pubblicità non richiesta,*
    - ✓ *Comunicazione a terzi diversi da Responsabile e Incaricati ,*
    - ✓ *Trasferimento dati extra UE*
    - ✓ *.....*
- **GRANULARITA'**
  - ***Richiesta Consenso distinto e separato per ciascuna finalità***

IL CONSENSO (3/4)

- **QUANDO DEVE ESSERE DISPONIBILE**
  - *Prima del trattamento*

- **IN CHE FORMA**
  - *In forma scritta . Se orale, va documentata*

- **DIMOSTRABILITA'**
  - *Il Titolare deve essere in grado di darne dimostrazione*
  - *Opportuno prevedere una modulistica, chiara e semplice*

New

- **DIRITTO DI REVOCA**
  - *Revocabile in qualsiasi momento*
  - *Il Titolare deve informare di ciò l'Interessato*

New

IL CONSENSO (4/4)

- **QUANDO E' NECESSARIO**
  - *Se non ricorre un altro caso di liceità previsto dal Regolamento*

- **QUANDO <u>NON</u> E' NECESSARIO: *CASI DI LICEITA' -art 6***
  - *Per i trattamenti necessari ad eseguire un contratto o per eseguire misure precontrattuali su richiesta dell'interessato*
  - *Per adempiere ad un obbligo legale*
  - *Per la salvaguardia degli interessi vitali dell'interessato o di altra persona*
  - *Per un compito di interesse pubblico*
  - New *Per il perseguimento del legittimo interesse del Titolare (salvo che non prevalgano i diritti fondamentali dell'interessato)*

New *in tali casi non va richiesto*

IL CONSENSO
PER IL MARKETING

- **ATTIVITA' DI MARKETING NON RICHIESTO**
  - *Le Regole sono contenute nella Direttiva UE sulle Comunicazioni elettroniche , recepite dal Codice Privacy, art 130 che rimane in vigore.*

- **COSA SI INTENDE PER MKTG NON RICHIESTO**
  - *Attività promozionale su iniziativa del Titolare*
  - *Eesempio : invio materiale pubblicitario e simili tramite e-mail , fax , SMS, Marketing telefonico e postale*

- **CONDIZIONE DI LICEITA'**
  - *Consenso espresso in varie forme, Diritto di Opposizione*

- **APPLICABILITA'**
  - *Non solo persone fisiche ma anche persone giuridiche*

IL DIRITTO DI CONTROLLO SUI PROPRI DATI

- **SCOPO**
  - *Dominio sui dati e Verifica di correttezza (art.15-22)*

- **COSA COMPRENDE**
  - *DIRITTO DI ACCESSO*
  - *DIRITTO DI RETTIFICA*
  - New *DIRITTO ALL' OBLIO*
  - New *DIRITTO DI LIMITAZIONE DEL TRATTAMENTO*
  - New *DIRITTO ALLA PORTABILITA' DEI DATI.*

Riscontro al Diritto d'Accesso - Art.12

- Mentre il Codice Privacy prevede 15 giorni di tempo (più ulteriori 15 in caso di complessità di reperimento di informazioni), il Regolamento Europeo aumenta il termine a 30 giorni, più ulteriori 30 giorni (2 mesi) in caso di complessità 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 e del numero di richieste.

In caso di dubbi circa l'identità della persona fisica, il Titolare del trattamento può richiedere ulteriori informazioni.

Le informazioni possono essere fornite in combinazione con icone standardizzate. L'Interessato è informato dei motivi del ritardo entro 30 giorni dal ricevimento della richiesta

Registro delle Opposizioni
Fondazione Ugo Bordoni
Robinson List

- Il Ministero dello sviluppo economico istituisce, ai sensi dell'articolo 130, comma 3-bis, del Codice, e sulla base delle disposizioni di cui all'articolo 4, il registro pubblico delle opposizioni

- La Fondazione Ugo Bordoni è un'Istituzione di Alta Cultura e Ricerca, sottoposta alla vigilanza del Ministero dello Sviluppo Economico. www.fub.it/
- http://www.registrodelleopposizioni.it/.

Minori Più Protetti – Art. 8

Il trattamento di dati personali di minori di età inferiore di minori al di sotto dei 16 anni - o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni - è lecito se e nella misura in cui il consenso è espresso o autorizzato dal genitore o dal tutore del minore.

Il Titolare del Trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia espresso o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

VIETATO ai MINORI

Uniformazione del concetto di «minore di anni 18»

Il trattamento dei Dati di minori ~~di anni 13~~ verrà subordinato al consenso da parte di un genitore

Modificato in: minori di 16 anni o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni

Profilazione – Art. 22 – Testo Definitivo

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona.

Tale articolo non si applica nel caso in cui la decisione:

Sia necessaria per la conclusione o l'esecuzione di un contratto.*

Sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il Titolare del trattamento.

Si basi sul consenso esplicito dell'Interessato.*

* In questi casi il Titolare del Trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, tra cui almeno il diritto di ottenere l'intervento umano da parte del Responsabile del Trattamento, di esprimere la propria opinione e di contestare la decisione.

Le decisioni basate sul trattamento automatizzato di dati personali destinato a valutare taluni aspetti della personalità dell'interessato non possono basarsi unicamente sulle categorie particolari di dati personali.

Principio di Minimizzazione – Art. 5

Testo Commissione LIBE: Il principio di minimizzazione dei dati prevede una raccolta, memorizzazione ed elaborazione di dati personali, solo se adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Raccolta

Conservazione

Elaborazione

Il testo della Commissione LIBE faceva riferimento a «Dati Limitati al Minimo Necessario»

Il testo del Consiglio Europeo eliminava tale principio, limitandolo a un «Dati Non Eccessivi»

Nel testo definitivo vengono introdotti «Dati Limitati a Quanto Necessario»

Diritto all'Oblio – Cancellazione dei Dati
Art. 17

L'Interessato ha il diritto di ottenere la cancellazione dei propri dati ~~e la rinuncia ad una ulteriore diffusione degli stessi~~.

Il Titolare del trattamento che rende pubbliche delle informazioni è tenuto a prendere tutte le misure ragionevoli, anche tecniche, per informare ~~i soggetti terzi, che a loro volta trattano tali dati,~~ i Titolari di un'eventuale richiesta di cancellazione da parte di un soggetto interessato, al fine di provvedere anch'essi all'eliminazione di qualsiasi link, copia o riproduzione dei dati personali.

~~Il Responsabile del trattamento è responsabile anche della pubblicazione dei dati effettuata da soggetti terzi, qualora siano stati autorizzati dallo stesso.~~

Corte di Giustizia Europea nella celebre sentenza "Google Spain/Inc. v. Agencia Española de Protección de Datos (AEPD)/Mario Costeja González" del 13 maggio 2014

New

IL DIRITTO ALL'OBLIO

- **COSA PUO' CHIEDERE L'INTERESSATO**
  - *CANCELLARE I DATI*
    - ✓ *se è esaurita la finalità del trattamento*
    - ✓ *se è stato revocato il Consenso*
    - ✓ *se è stata fatta Opposizione al trattamento*
    - ✓ *se trattati in violazione di legge.*

- **RAFFORZAMENTO PER INTERNET**
  - *OBBLIGO DEL TITOLARE "EDITORE" DEI DATI*
    - ✓ *Informare altri Titolari di cancellare i link*

Diritto all'Oblio – Casi di Esclusione

Il diritto alla cancellazione non si applica qualora il trattamento dei dati sia necessario per:

Libertà di Espressione e di Informazione

Adempimento Obblighi Legali

Interesse Pubblico in ambito Sanitario

Interesse Storico, Scientifico, Statistico

Difesa di un Diritto in Sede Giudiziaria

L'Interessato ha il diritto di ottenere la limitazione del trattamento dei dati nei seguenti casi:

Contestazione dell'esattezza dei Dati

Trattamento Illecito dei Dati (se richiesto)

Difesa di un Diritto in Sede Giudiziaria

In Caso di Opposizione al Trattamento

Diritto all'Oblio – Portabilità dei Dati

Art. 20

Diritto per il soggetto Interessato di ricevere dal Titolare del trattamento copia dei propri dati personali, in formato elettronico strutturato, di uso comune e leggibile a macchina, al fine di consentirgli ~~un ulteriore agevole utilizzo~~ la trasmissione ad un altro Responsabile del trattamento.

Il testo definitivo introduce per l'Interessato il diritto di ottenere la trasmissione diretta dei dati da un Titolare del trattamento ad un altro, se tecnicamente fattibile.

Si tratta di un diritto che non è applicabile ai Titolari del trattamento (società) rispetto all'allocazione di dati su sistemi di soggetti terzi (cloud). Tale diritto è riconosciuto, infatti, solamente ai soggetti Interessati per la tutela dei propri dati personali.

New

IL DIRITTO ALLA PORTABILITA' DEI DATI

- **OBIETTIVO**
  - *SEMPLIFICARE CAMBIO DI FORNITORE*
- **QUANDO PUO' ESERCITARE IL DIRITTO**
  - *In caso di trattamento necessario per eseguire contratto*
  - *In caso di dati basati su Consenso*
- **COSA PUO' CHIEDERE L'INTERESSATO**
  - *IN CASO DI TRATTAMENTO AUTOMATIZZATO*
    - ✓ *Ricevere i dati in formato chiaro e leggibile*
    - ✓ *Ottenere il trasferimento automatico ad altro Fornitore, ove fattibile.*

New

IL DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

- **COSA PUO' CHIEDERE L'INTERESSATO**
  - *LIMITARE IL TRATTAMENTO*
    - ✓ *In caso di dati inesatti, fino alla rettifica*
    - ✓ *In caso di contestazione, fino a chiarimento*
    - ✓ *Su richiesta, in alternativa alla cancellazione*

- **OBBLIGO DEL TITOLARE: DEFINIRE LA MODALITA'**
  - ✓ *Trasferire i dati ad altro sistema*
  - ✓ *Rendere i dati inaccessibili*
  - ✓ *Rimuovere temporaneamente i dati*
  - ✓ *Congelare i dati*
  - ✓ *In ogni caso, identificarli nel sistema*

Aziende Extra UE – Capo V

Il Regolamento Europeo impone che si applichi la normativa UE qualora un "Azienda Extra-CEE" rivolga servizi o prodotti al mercato UE.

Ciò significa che un'impresa non europea che opera nell'ambito dell'unione sarà tenuta a rispettare e a recepire integralmente i nuovi obblighi introdotti dalla riforma e a garantire lo stesso livello di tutela e riservatezza delle informazioni di una qualunque azienda europea.

Trasferimento Extra-CEE dei Dati

Qualunque organizzazione con sede al di fuori dell'Unione Europea che tratti dati derivanti dalle filiali europee sarà tenuto a farlo nel rispetto totale del nuovo regolamento, applicando gli stessi principi e recependo gli stessi obblighi previsti per trattamenti effettuati nella stessa UE.

Trasferimento Extra-CEE

Rispettando il Regolamento Europeo

Via libera ai trasferimenti di dati verso Paesi terzi, anche se sprovvisti di una legge sulla protezione dei dati, attraverso la predisposizione di codici di condotta e accordi, come ad esempio le BCR (Binding Corporate Rules), Safe Harbor (ad esclusione degli USA) e UE-USA Privacy Shield.

“Obblighi del Titolare del Trattamento”

Data Protection Impact Assessment – Art. 35

Quando il trattamento, per la sua natura, campo di applicazione, contesto o finalità, presenta rischi ~~specifici~~ elevati per i diritti e le libertà ~~degli interessati~~ di persone fisiche, il Titolare del Trattamento è tenuto ad effettuare una valutazione dell'impatto del trattamento previsto sulla protezione dei dati personali.

DATA	N° RIF	OGGETTI SOTTOPOSTI A CONTROLLO	CONFORMITÀ	NOTE SULLA CONFORMITÀ	IMPATTO DEL RISCHIO	INDICE DEL RIS			SANZIONE
15/09/14	01.01	**Individuazione del Titolare del Trattamento dei dati**	**Conforme**	Nei casi in cui tutti i poteri e le responsabilità derivanti dall'esercizio di un'attività non siano in capo ad un unico vertice (es. Amministratore unico) si rende necessario individuare un soggetto che rivesta la figura del Titolare del Trattamento dei dati con poteri di delega e di firma.	Rischio di mancata Identificazione del Titolare del Trattamento di dati che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.	1	1	1	Omessa Adozione di Misura Minima di Sicurezza **Arresto sino a due anni, Sanzione Amministrativa da € 10.000 a 120.000**
15/09/14	01.02	**Nomina dei Responsabili e degli Incaricati al Trattamento dei dati**	**Parzialmente conforme**	Sono stati designati gli Incaricati al Trattamento dei dati, ma non sono stati nominati i Responsabili del Trattamento. Nomina Responsabile della Sicurezza dei dati e del Trattamento:ASSENTI. Le lettere di incarico sono state redatte e risultano essere conformi.	Rischio di mancata Identificazione del Personale interno ad esterno preposto allo svolgimento di compiti specifici e relativi Trattamenti di dati.	2	3	6	Omessa Adozione di Misura Minima di Sicurezza **Arresto sino a due anni, Sanzione Amministrativa da € 10.000 a 120.000**
15/09/14	01.04	**Identificazione dei Responsabili al Trattamento in Out-Sourcing**	**Non Conforme**	Non sono stati identificati i Responsabili al Trattamento dei dati in Out--Sourcing con relativa nomina.	Rischio di mancata Identificazione dei Responsabili in Out-Sourcing preposti a Specifici Trattamenti dei dati.	3	3	9	Omessa Adozione di Misura Minima di Sicurezza **Arresto sino a due anni, Sanzione Amministrativa da € 10.000 a 120.000**

Data Protection Impact Assessment – Art. 35

La valutazione è richiesta in particolare nei seguenti casi:

Profilazione o valutazione di aspetti personali che influiscono su decisioni con effetti giuridici o incidono su persone fisiche

Trattamento su larga scala di Dati Particolari o relativi a condanne penali

Sorveglianza sistematica di zona accessibile al pubblico su larga scala

L'Autorità di controllo redige e rende pubblico l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

Data Protection Impact Assessment-Art. 35

La valutazione deve contenere almeno:

Descrizione sistematica dei trattamenti e delle finalità

Valutazione su necessità e proporzionalità dei trattamenti

Valutazione di rischi per i diritti e le libertà degli interessati

Misure previste per affrontare i rischi