GITTI AND PARTNERS

LE NOVITÀ DEL GDPR, CON PARTICOLARE RIFERIMENTO ALLA TUTELA DELLA *PRIVACY* IN AMBITO BANCARIO, FINANZIARIO E ASSICURATIVO E AL RELATIVO APPARATO SANZIONATORIO

15 MARZO 2018

Avv. Paola Sangiovanni
Partner
Gitti and Partners - Studio Legale Associato

GDPR, Come e Perché

- Il Regolamento GDPR è direttamente applicabile in tutti gli Stati membri dal 25 maggio 2018.

- La *ratio*:

  - Impedire la frammentazione della normativa nazionale e favorire la **certezza del diritto**;

  - Creare un **mercato unico digitale** e sostenere la *digital economy* europea;

  - Scongiurare «*the end of privacy*» dell'era digitale, creando un clima di fiducia negli interessati a fronte di (e nonostante) le **innovazioni tecnologiche** che utilizzano un numero infinitamente maggiore di dati personali.

LE OPPORTUNITÀ DELL'ERA DIGITALE.
LA **PROFILAZIONE:** UNO STRUMENTO PER **PREVEDERE**

- **Profilazione**: qualsiasi forma di **trattamento automatizzato** di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per **analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.**

- **Diritto di opposizione dell'interessato alla profilazione.** 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 in modo analogo significativamente sulla sua persona (art. 22 del Regolamento).

IL RISCHIO NELL'ERA DIGITALE

- Non occorrono dati particolarmente «sensibili», basta incrociare dati non personali per ottenere informazioni riservate e molto dettagliate sulle persone;

- Con l'era dei *big data,* questo contesto «*data intensive*» crea rischi molto maggiori per i dati personali e per i diritti degli interessati;

- Il GDPR si incentra proprio sul RISCHIO: mentre la Direttiva previgente si focalizzava sui diritti dell'interessato, il GDPR impone al titolare un'analisi dei rischi («*risk assessment*») a cui sono sottoposti i dati, e impone **misure tecniche e organizzative adeguate al livello di rischio**.

- Si assiste ad una forte responsabilizzazione del titolare del trattamento dei dati, che non solo deve applicare la norma, ma deve valutare i rischi e adottare misure appropriate.

QUALI MISURE?

- **Misure tecniche** per proteggere i dati contro perdite o furti

- **Misure organizzative:**
  - *Data governance*
  - *Data Protection Officer*
  - Formazione
  - Procedure:
    - *Data breach policy;*
    - *Data retention policy;*
    - *Subject access request policy;*
    - *Data protection policy;*

PSEUDOANONIMIZZAZIONE: UNA MISURA TECNICA E ORGANIZZATIVA

DATO PERSONALE: «***qualsiasi informazione riguardante una persona fisica identificata o identificabile*** *(«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»*

PSEUDOANONIMIZZAZIONE: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

I Principi da Rispettare

- **liceità,**
- correttezza,
- trasparenza,
- limitazione della finalità,
- **minimizzazione dei dati,**
- esattezza,
- **limitazione della conservazione,**
- integrità,
- responsabilizzazione

PRINCIPIO DI LICEITÀ

- Il trattamento è lecito se:
  - **L'interessato ha espresso il proprio consenso (esplicito, informato e per specifiche finalità);**
  - **Necessario per l'esecuzione di un contratto di cui l'interessato è parte;**
  - **Necessario per adempiere un obbligo legale;**
  - Necessario per la salvaguardia degli interessi vitali;
  - Necessario per l'esecuzione di un compito di interesse pubblico;
  - Necessario per il perseguimento del legittimo interesse del titolare o di terzi, se non prevalgono i diritti dell'interessato.

In Italia: In Attesa del Decreto Legislativo…

Legge	Entrata in vigore	Articolo	Oggetto	Termine per esercizio delega
25 ottobre 2017, n. 163 **Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017.**	21 novembre 2017	13	Il Governo è delegato ad adottare uno o più decreti legislativi per l'adeguamento della normativa italiana al GDPR. Nell'esercizio della delega, il Governo dovrà: a) abrogare espressamente le disposizioni del Codice Privacy incompatibili con il GDPR; b) modificare il Codice Privacy, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel GDPR; c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni del GDPR; d) prevedere il ricorso a specifici provvedimenti attuativi e integrativi del Garante; e) adeguare il sistema sanzionatorio penale e amministrativo alle disposizioni del GDPR	21 maggio 2018
20 novembre 2017, n. 167 **Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017.**	12 dicembre 2017	28	a) Modifiche all'articolo 29 del Codice Privacy sul ruolo e sui requisiti del responsabile del trattamento a) Introduzione dell'Art. 110-bis del Codice Privacy per il riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici ("Nell'ambito delle finalità di ricerca scientifica ovvero per scopi statistici può essere autorizzato dal Garante il riutilizzo dei dati, anche sensibili, ad esclusione di quelli genetici, a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela degli interessati").	N.A.

CON LO SPETTRO DI SANZIONI VOLUTAMENTE SPAVENTOSE!

Sanzioni amministrative pecuniarie fino a **Euro 20 milioni** o, se superiore, fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente, in caso di violazione:

- Dei principi base del trattamento (liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, responsabilizzazione)
- Dei diritti degli interessati, incluso il diritto all'oblio e alla portabilità
- Delle regole per il trasferimento dei dati all'estero
- Dei provvedimenti delle Autorità di controllo

GRAZIE PER L'ATTENZIONE!

Quindi:

- Dati come opportunità («*data is the new oil*»)
- Trattamento dati personali = attività pericolosa!

Domande?

paola.sangiovanni@grplex.com

MILANO
Via Dante, 9

LONDRA
71, Central Street

BRESCIA
Piazza della Loggia, 5

www.grplex.com

GITTI AND PARTNERS