General Data Protection Regulation

«GDPR»

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

EBAS
e-business association

Milano

Alan M. Rhode

Alan.rhode@taxmen.eu

13 febbraio 2018

La riforma della privacy

- **25 maggio 2018**: entra in vigore, in tutta **Europa**, la nuova normativa a **tutela** dei dati personali e della loro **libera circolazione** (Reg. UE 679/2016 – «**GDPR»**).
- Il GDPR andrà a **abrogare** o **integrare** le attuali normative privacy nazionali (ad oggi «soltanto» armonizzate in base alla **Direttive 95/46/EC**).
- Entro la fine del 2018 dovrebbe, inoltre, essere approvato il **Regolamento e-Privacy**, che disciplina la privacy nell'ambito delle **comunicazioni elettroniche**.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Principali modifiche

- Tra le **molteplici novità**, il GDPR introduce:
  - ✓ **Amplia** spettro territoriale;
  - ✓ **Nuovi diritti** per gli interessati (e.g., diritto all'oblio, diritto alla portabilità dei dati, etc.);
  - ✓ **Maggiori requisiti** per la validità del **consenso**;
  - ✓ Concetto di **privacy by design**;
  - ✓ Obbligo di notifica in caso di **data breach**;
  - ✓ Obbligo di nomina di **DPO**;
  - ✓ Obbligo di espletamento di **DPIA**;
  - ✓ **Sanzioni** più onerose per violazioni.

Dati personali

- Il GDPR disciplina il trattamento **automatizzato** di **dati personali**.
- La definizione di dati personali è similare rispetto a quella già inclusa nella **Direttiva UE 46/1995**.
- **Dati personali**: ogni informazione riguardante una persona fisica **identificata** o **identificabile**.
- **Identificabile**: la persona che può essere identificata, **direttamente/indirettamente**, con specifico riferimento a identificativi quali nome, numero identificativo, dati relativi all'ubicazione, **identificativi online** oppure elementi caratteristici della sua identità…

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Dati personali (2)

- I **dati anonimi** non rientrano nell'ambito di applicazione del GDPR.
- Incentivata la **pseudonimizzazione**: «*può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati*» (Considerando nr. 89).
- Specifiche regole riguardano i **dati sensibili**.

Principi del trattamento

- I dati personali devono essere:
  a) trattati in modo **lecito**, corretto e **trasparente**;
  b) raccolti e trattati per **finalità** determinate, esplicite e legittime;
  c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
  d) esatti e, se necessario, **aggiornati**;
  e) conservati per un **tempo non superiore** a quanto necessario;
  f) trattati garantendo adeguata **sicurezza**.

Liceità del trattamento

- Il trattamento dei dati è **lecito** quando sussiste almeno uno dei seguenti **requisiti**:

  a) Consenso dell'interessato;

  b) Adempimento **obblighi contrattuali**;

  c) interessi vitali della persona interessata o di terzi;

  d) obblighi di **legge** cui è soggetto il titolare;

  e) interesse pubblico o esercizio di pubblici poteri;

  f) interesse legittimo prevalente del titolare o terzi a cui i dati vengono comunicati.

Il consenso

- Il **consenso** dell'interessato può essere posto a fondamento del trattamento di dati personali **soltanto** quando è:

  1. **Espresso liberamente**;
  2. Specifico («**granulare**»);
  3. **Informato**;
  4. Manifestazione di **volontà** dell'interessato, con cui quest'ultimo manifesta il proprio assenso, mediante dichiarazione o **azione positiva inequivocabile**, al trattamento dei suoi dati personali.

Consenso informato

- L'**Article 29 Working Party** ha indicato i requisiti minimi di un'informativa affinché il consenso possa ritenersi informato (doc. 259 del 28 novembre 2017):

3.3.1. Minimum content requirements for consent to be 'informed'

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 is of the opinion that at least the following information is required for obtaining valid consent:

(i) the controller's identity,

(ii) the purpose of each of the processing operations for which consent is sought[30],

(iii) what (type of) data will be collected and used, [31]

(iv) the existence of the right to withdraw consent,[32]

(v) information about the use of the data for decisions based solely on automated processing, including profiling, in accordance with Article 22 (2)[33], and

(vi) if the consent relates to transfers, about the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards (Article 49 (1a)). [34]

Forma del Consenso

- Il **consenso** al trattamento dei dati personali può essere **costituito** da una dichiarazione espressa o da un'azione che lo manifesti in modo **inequivocabile**.

However, within the requirements of the GDPR, controllers have the liberty to develop a consent flow that suits their organisation. In this regard, physical motions can be qualified as a clear affirmative action in compliance with the GDPR.

[Example 12]
Swiping on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.

[Example 13]
Scrolling down or swiping through terms and conditions which include declarations of consent (where a statement comes up on screen to alert the data subject that continuing to scroll will constitute consent) will not satisfy the requirement of a clear and affirmative action. This is because the alert may be missed where a data subject is quickly scrolling through large amounts of text and such an action is not sufficiently unambiguous.

Prova del consenso

- Il data controller deve reperire/mantenere **evidenza** del consenso dell'interessato: «*Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare chel'interessato ha prestato il proprio consenso al trattamento dei propri dati personali*».

- Il GDPR **non** indica la forma di tale prova.

- La **prova** del consenso deve essere mantenuta fino a che non si prescrive il diritto dell'interessato ad agire nei confronti del controller per violazioni di privacy oppure fino a quando vi è un'obbligazione legale.

Consenso dei minori

- Il GDPR inserisce **limiti stringenti** al consenso dei **minori** quale fondamento per la liceità del trattamento dati in **ambito online**.

- Sedici (16) è l'**età minima** per fornire il proprio consenso al trattamento dati online. Sotto tale età, il consenso è valido soltanto se prestato da **genitori** o tutori.

- Il GDPR permette ai singoli stati UE di abbassare tale soglia fino a **tredici (13) anni**.

Informative e privacy policy

- Il GDPR **accresce** gli **oneri informativi** a carico del data controller. In particolare, oltre a quanto previsto dalla normativa in vigore, bisognerà anche indicare nelle informative:
  - ✓ Modalità per contattare il DPO, ove presente;
  - ✓ Eventuali interessi legittimi su cui si fonda il trattamento;
  - ✓ Trasferimenti di dati verso territori extra-UE;
  - ✓ Periodo di ritenzione dati (ove non possibile a priori, il criterio per determinarlo);
  - ✓ I «nuovi» diritti (diritto all'oblio, diritto alla sospensione del trattamento, diritto alla portabilità dei dati, etc.)
  - ✓ Facoltà di presentare esposti presso autorità competente;
  - ✓ Eventuali obblighi contrattuali/legali a fornire dati personali.

Diritto alla portabilità

- L'interessato ha il **diritto di ricevere** dal data controller i propri dati personali e ha il diritto di trasmettere tali dati a un altro data controller senza impedimenti quando:

  a) il trattamento si basi sul **consenso** o su un **contratto**; e, inoltre,

  b) il trattamento sia effettuato con **mezzi automatizzati**.

- Il controller deve trasmettere i dati «*in un **formato** strutturato, di uso comune e leggibile da dispositivo automatico*».

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Diritto all'oblio (1)

- L'interessato ha il diritto di ottenere la **cancellazione** dei propri dati personali **senza ingiustificato ritardo** da parte del controller ove sussista uno dei seguenti tali motivi:

  a) i dati personali **non** sono più **necessari** per le finalità in base a cui sono raccolti o trattati;

  b) revoca del consenso;

  c) opposizione al trattamento;

  d) illiceità del trattamento;

  e) obbligo legale di cancellazione;

  f) i dati personali sono stati raccolti per l'offerta di servizi della **società dell'informazione**.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Diritto all'oblio (2)

- Se ha reso pubblici dei dati personali e ha ora l'obbligo di cancellarli, il controller deve adottare le misure ragionevoli, tenendo conto di tecnologia disponibile e costi, per **informare** altri (eventuali) data controller sulla richiesta dell'interessato di cancellare i dati personali.

- Il GDPR prevede alcune limitazioni al **diritto all'oblio**: per esempio, ove il trattamento di tali dati personali sia necessario per l'esercizio del diritto alla libertà di espressione/informazione ovvero per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Data Protection Officer (DPO)

- La nomina di un DPO è **obbligatoria** in tre casi:
  1. Il trattamento è compiuto da **autorità pubblica** o organismo pubblico, salvo autorità giurisdizionali; o
  2. le **attività principali** di data controller e/o data processor consistono in trattamenti che, per loro natura, ambito d'applicazione e/o finalità, richiedono il **monitoraggio regolare+sistematico** degli interessati **su larga scala**; oppure
  3. le **attività principali** di data controller e/o data processor consistono nel trattamento, **su larga scala**, di **dati sensibili** o relativi a condanne penali/ reati.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Data Protection Officer (DPO) - 2

- Il GDPR adotta locuzioni **ambigue** per individuare le condizioni di nomina obbligatoria del DPO: "*attività principali…larga scala…monitoraggio regolare e sistematico*".

- Secondo l'A29 Working Party, la gestione delle "buste paga" o l'utilizzo di ordinari strumenti informatici da parte dell'impresa **non** rappresentano attivitá principali in coincidenza delle quali sorge l'obbligo di nomina del DPO, bensí **accessorie**.

On the other hand, all organisations carry out certain activities, for example, paying their employees or having standard IT support activities. These are necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Data Protection Officer (DPO) - 3

- Secondo l'Article 29 Working Party, le seguenti attività implicano il trattamento di dati personali su **larga scala**:

Examples of large-scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

Data Protection Officer (DPO) - 4

- Secondo l'Article 29 Working Party, esempi di attività che implicano **monitoraggio regolare+sistematico** di soggetti interessati sono:

Examples: operating a telecommunications network; providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.

Data Protection Officer (DPO) - 5

- Il DPO può appartenere all'**organico** dell'impresa o essere **esterno**. In ogni caso, bisogna porre attenzione ai potenziali **conflitti d'interesse** (e.g., no marketing manager, IT manager, etc.).

- La presenza di un DPO deve essere indicate in privacy policy e notificata all'autorità competente.

- Il DPO deve possedere sufficienti **conoscenze** in ambito privacy e svolgere una costante attività d'**aggiornamento**.

Data Protection Officer (DPO) - 6

- L'impresa deve assicurarsi che il DPO sia "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".

- Il DPO **non** deve ricevere alcuna **istruzione** per quanto riguarda l'esecuzione dei propri compiti; non è rimosso o penalizzato dall'impresa per l'adempimento dei propri compiti.

- Il DPO deve riferire **direttamente** al **vertice gerarchico** dell'impresa.

Data Protection Officer (DPO) - 7

- **Principali funzioni** del DPO:

1. **fornire informazioni** all'impresa sugli obblighi di legge relativi alla protezione dei dati;
2. **sorvegliare** il rispetto degli obblighi legali e delle politiche aziendali in materia di privacy, compresi attribuzione di responsabilità e formazione del personale;
3. fornire, ove richiesto, un parere in merito alla **DPIA** e sorvegliarne lo svolgimento;
4. **cooperare** con e fungere da punto di **contatto** per l'**autorità di controllo**.

Data Privacy Impact Assessment (DPIA)

- Il DPIA è un **audit preventivo** teso a valutare l'**impatto** di uno o più trattamenti dati sui **diritti privacy** degli interessati.

- La nuova normativa **impone** l'espletamento di un DPIA ove il trattamento possa «*presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche*» (art. 35).

- Il DPIA ha la funzione di **prevenire** i data breach e di dimostrare il rispetto della normativa privacy da parte del data controller/processor («***accountability***»).

Data Privacy Impact Assessment (DPIA) - 2

- Il GDPR indica **alcuni casi** in cui il DPIA deve ritenersi **obbligatorio**. Per esempio, quando un'organizzazione svolga:

1. una **valutazione sistematica e globale** di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la **profilazione**, e su cui si fondano decisioni con effetti giuridici o analoghi sugli interessati;
2. il trattamento, su larga scala, di **dati sensibili** e di dati relativi a condanne penali e a reati;
3. la sorveglianza sistematica e su larga scala di **zona accessibile** al pubblico.

Data Privacy Impact Assessment (DPIA) - 3

- Secondo l'A29 Working Party, alcuni esempi di attività che dovrebbero essere soggette a DPIA sono:

Examples of processing	Possible Relevant criteria	DPIA required?
A hospital processing its patients' genetic and health data (hospital information system).	- Sensitive data - Data concerning vulnerable data subjects	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	- Systematic monitoring - Innovative use or applying technological or organisational solutions	
A company monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	- Systematic monitoring - Data concerning vulnerable data subjects	
The gathering of public social media profiles data to be used by private companies generating profiles for contact directories.	- Evaluation or scoring - Data processed on a large scale	
An online magazine using a mailing list to send a generic daily digest to its subscribers.	- (none)	Not necessarily
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on past purchases behaviour on certain parts of its website.	- Evaluation or scoring, but not systematic or extensive	

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Data Privacy Impact Assessment (DPIA) - 3

- **Contenuto minimo** di un DPIA:

a) descrizione sistematica dei trattamenti previsti e delle loro finalità, compreso, ove applicabile, l'interesse legittimo perseguito dal data controller;
b) valutazione di necessità e proporzionalità dei trattamenti;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare tali rischi, includendo le garanzie, misure di sicurezza e meccanismi per garantire la protezione dei dati personali.

Data breach

- Il GDPR introduce stringenti **obblighi di notifica** in capo a data controller/processor nel caso di **data breach**.

- «Data breach»: «*la* ***violazione*** *di* ***sicurezza*** *che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*» (art. 4).

- Nel caso in cui la data breach riguardi il **data processor**, quest'ultimo deve notificare la violazione al proprio data controller senza ingiustificato ritardo.

Data breach (2)

- A sua volta, il data controller deve notificare la violazione all'**autorità di controllo** competente senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, «***a meno che*** *sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*» (art. 33).

Data breach (3)

- Quando la violazione presenta un **rischio elevato** di danno ai diritti degli interessati, il data processor deve tempestivamente comunicare loro la violazione.

- **Esenzioni**:

  a) il data controller ha messo **preventivamente** in atto misure tecnico-organizzative adeguate per proteggere i dati personali oggetto di violazione; o

  b) il data controller ha **successivamente** adottato misure atte a scongiurare un rischio elevato per i diritti e le libertà degli interessati; oppure

  c) la comunicazione richiede **sforzi sproporzionati**.

Trasferimento di dati verso extra-UE

- Il GDPR pone **restrittive limitazioni** al trasferimento di dati personali fuori dall'EEA.

- Il trasferimento è permesso soltanto ove, in particolare, uno dei seguenti requisiti sia soddisfatto:

  ✓L'UE ha deciso che lo stato terzo garantisce un adeguato livello di protezione;

  ✓Consenso dell'interessato;

  ✓Necessità contrattuale

  ✓Tutela di diritti;

  ✓Importanti ragioni d'interesse pubblico;

  ✓Standard contrattuali con processor non-UE.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE