



UGHI E NUNZIANTE

Gli obblighi cross-border previsti dal GDPR

Avv. Massimiliano Pappalardo

18 marzo 2021



**SWISS
CHAMBER**

Camera
di Commercio
Svizzera
in Italia

Ambito di applicazione del GDPR: Territorio

1. Imprese stabilite nel territorio UE

2. Imprese extra UE

- che **offrono** (anche a titolo gratuito) servizi o prodotti a persone che si trovano nel territorio UE, o
- che **monitorano** i comportamenti di interessati che si trovano nell'UE.

Cosa si intende per Stabilimento?

«[l]o stabilimento implica l'**effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile**. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica» (Considerando 22 GDPR).

Cosa si intende per Targeting?

«[p]er determinare se il titolare o il responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione» (Considerando 23 GDPR).

Lo stesso considerando specifica ulteriormente che:

« (...) l'utilizzo di una **lingua** o di una **moneta abitualmente utilizzata in uno o più Stati membri**, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione».

Linee-guida 3/2018 dello European Data Protection Board sull'ambito di applicazione territoriale del GDPR

Example 16: A Swiss University in Zurich is launching its Master degree selection process, by making available an online platform where candidates can upload their CV and cover letter, together with their contact details. The selection process is open to any student with a sufficient level of German and English and holding a Bachelor degree. The University does not specifically advertise to students in EU Universities, and only takes payment in Swiss currency.

As there is no distinction or specification for students from the Union in the application and selection process for this Master degree, it cannot be established that the Swiss University has the intention to target students from a particular EU member states. The sufficient level of German and English is a general requirement that applies to any applicant whether a Swiss resident, a person in the Union or a student from a third country. Without other factors to indicate the specific targeting of students in EU member states, it therefore cannot be established that the processing in question relates to the offer of an education service to data subject in the Union, and such processing will therefore not be subject to the GDPR provisions.

The Swiss University also offers summer courses in international relations and specifically advertises this offer in German and Austrian universities in order to maximise the courses' attendance. In this case, there is a clear intention from the Swiss University to offer such service to data subjects who are in the Union, and the GDPR will apply to the related processing activities.

La nomina di un rappresentante UE

È previsto l'obbligo di designazione per iscritto di un rappresentante stabilito nell'UE per **Titolari** e **Responsabili** stabiliti in Paesi extra-UE a cui si applichi il Regolamento (art. 27 GDPR)

One Stop Shop

Quali sono per una società extra UE i vantaggi di avere uno **stabilimento** sul territorio dell'Unione Europea?

Autorità di Controllo Capofila:

è l'autorità dello stabilimento principale o unico nell'UE del titolare o responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre autorità di controllo per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile.

Le Basi Giuridiche del GDPR

Il trattamento – ai sensi del GDPR - è lecito solo se e nella misura in cui ricorra una valida base giuridica, tra cui:

- l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per **la salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per il perseguimento del **legittimo interesse del titolare del trattamento** o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali.

Il Responsabile del Trattamento: Quali differenze tra GDPR e nuova LPD

- **Responsabile del Trattamento:** La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
 - Identità dei principi tra GDPR e LPD
 - Regolamentazione più dettagliata da parte del GDPR

Il Responsabile del Trattamento: la designazione

I rapporti tra titolare e responsabile vanno regolati attraverso un **Contratto Scritto**:

- **Criteri di Designazione:**

- Qualora un trattamento debba essere effettuato per conto del titolare, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino **garanzie sufficienti** per mettere in atto **misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
- La rilevanza dei **Codici di Condotta** e dei **Meccanismi di Certificazione**

Il Responsabile del Trattamento: i compiti

- Esegue le istruzioni impartite dal titolare del trattamento
- Garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza
- Adotta tutte le misure di sicurezza necessarie
- Assiste il titolare del trattamento con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del titolare del trattamento di garantire l'esercizio dei diritti dell'interessato
- Assiste il titolare del trattamento nelle attività relative al **Data Protection Impact Assessment** e alla **Data Breach Notification**
- Su indicazione del titolare del trattamento, cancella o restituisce tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento
- Mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi a lui spettanti e contribuisce alle attività di revisione, comprese le ispezioni, effettuate, direttamente o indirettamente, dal titolare del trattamento

Data Protection Officer (DPO) Vs. Consulente per la Protezione dei Dati (CPD)

- **DPO** e **CPD** sono entrambe figure indipendenti provviste di competenze tecniche

- La nomina del **DPO** in alcuni casi è obbligatoria
- Il **DPO** svolge anche funzioni di controllo

Il Data Protection Officer

- La nomina del **DPO** è obbligatoria quando:

- le **attività principali** del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- le **attività principali** del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali.

Il Data Protection Officer: i requisiti

1 deve possedere **un'adeguata conoscenza specialistica** della normativa e delle prassi di gestione dei dati personali in relazione agli specifici trattamenti effettuati dal titolare o dal responsabile

2 deve adempiere ai suoi compiti in **piena indipendenza** e in assenza di conflitti di interesse

3 può essere un **dipendente del titolare** o del responsabile oppure assolvere i suoi compiti in base a un **contratto di servizi** (DPO interno/DPO esterno)

4 deve essere dotato dal titolare o dal responsabile delle **risorse umane e finanziarie** necessarie all'adempimento dei suoi compiti

I Diritti degli Interessati previsti dal GDPR

Trasparenza

Accesso

Rettifica

Cancellazione (Diritto all'Oblio)

Limitazione del trattamento

Portabilità

L'Impianto Sanzionatorio del GDPR

Le sanzioni amministrative pecuniarie previste dal **GDPR** possono arrivare:

- fino a **20 milioni di Euro**, oppure
- fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore

Grazie!

Avv. Massimiliano Pappalardo