ASSINDUSTRIA VENETOCENTRO
IMPRENDITORI PADOVA TREVISO

UNIS&F

GDPR (UE) 2016/679: A CHE PUNTO SIAMO?

Un anno dall'applicazione del GDPR: luci ed ombre

Pasquale Costanzo – Responsabile compliance privacy UNIS&F

Treviso, 23 maggio 2019

ASSINDUSTRIA VENETOCENTRO
IMPRENDITORI PADOVA TREVISO

UNIS&F

L’obiettivo è quello di eseguire un primo bilancio applicativo della normativa in materia di protezione dei dati personali, il tutto ad un anno (25 maggio 2018) dalla prima attuazione del Regolamento UE 2016/679 («GDPR»).

L’occasione è, dunque, quella di verificare «sul campo» ciò che sta accadendo in concreto all’interno del mondo aziendale, in termini di impatto della nuova normativa sulle strategie e sui processi organizzativi delle varie organizzazioni, verificando quelle che sono state le best practices fin qui adottate, evidenziando anche gli errori ad oggi commessi nell’applicazione della nuova normativa.

ASSINDUSTRIA VENETOCENTRO
IMPRENDITORI PADOVA TREVISO

UNIS&F

Osservatorio UNIS&F
Circa 3600 aziende associate

UNIS&F ogni anno attiva più di **200 commesse** (grandi aziende, PMI, organismi sanitari privati e pubblici, etc.)

Partecipazione con proprio personale al gruppo tecnico privacy di Confindustria, la cui mission è monitorare gli iter legislativi che hanno un impatto sulla materia della protezione dei dati personali.

Regolarmente si realizzano convegni e seminari specialistici. Ultimamente organizzati 2 master dedicati alla figura del DPO, nonché un recentissimo convegno riguardante il trattamento dei dati personali in ambito sanitario lo scorso 14 maggio.

ASSINDUSTRIA VENETOCENTRO
IMPRENDITORI PADOVA TREVISO

UNIS&F

Novità del Regolamento

1. Principio di *accountability* («responsabilizzazione»)
2. Data protection officer (DPO)
3. Approccio risk-based
4. Dimensione europea

ASSINDUSTRIA VENETOCENTRO
IMPRENDITORI PADOVA TREVISO

UNIS&F

1. Principio di *accountability* («responsabilizzazione»)

Il titolare del trattamento dei dati personali (e il responsabile) è tenuto ad adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

(Linee guida Garante privacy)

Cambio di rotta rispetto al passato: sono i titolari che decidono autonomamente le modalità, i limiti e le misure di sicurezza relative al trattamento dei dati personali (sempre nel rispetto del Regolamento e in ottemperanza di alcuni principi specifici contenuti in esso!). Approccio pratico e concreto alla disciplina in tema di protezione dei dati personali.

2. Data protection officer (DPO)

Elemento-chiave all'interno del nuovo sistema di *governance* dei dati: il «responsabile della protezione dei dati» (RPD) è finalizzato a facilitare l'attuazione del Regolamento da parte del titolare e/o del responsabile, riflettendo perciò l'approccio responsabilizzante del GDPR.

Il DPO/RPD svolge un ruolo di garanzia all'interno della *governance* privacy: punto di contatto tra Autorità di controllo, titolare e/o responsabile ed interessati.

ASSINDUSTRIA VENETOCENTRO
IMPRENDITORI PADOVA TREVISO

UNIS&F

3. Approccio risk-based

Il titolare del trattamento è tenuto a condurre un adeguato risk assessment, anche attraverso un apposito processo di valutazione, in modo da evidenziare i rischi privacy in cui è possibile incappare durante i processi di trattamento.

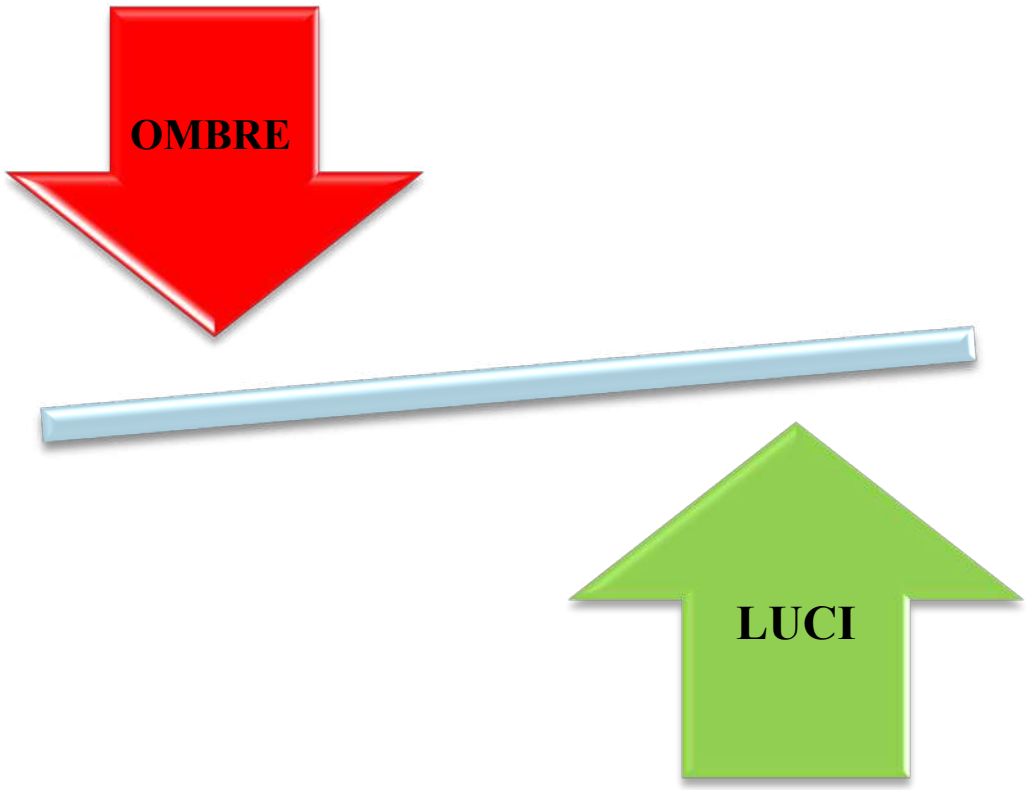
In questa direzione procedono le previsioni regolamentarie relative alla Data Protection Impact Assessment (DPIA), ossia una valutazione d'impatto privacy, richiesta per trattamenti su larga scala e le *misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio* (art. 32, par. 1, GDPR) che titolare e/o responsabile devono mettere in atto a seconda delle caratteristiche, in senso lato, del trattamento.

ASSINDUSTRIA VENETOCENTRO
IMPRENDITORI PADOVA TREVISO

UNIS&F

4. Dimensione europea

Il GDPR non riguarda solo il diritto alla protezione dei dati personali, ma la libertà di circolazione dei dati all'interno dell'Unione europea. Si applica in tutta Europa ed ogni singolo cittadino italiano o straniero può rivolgersi alla sua Autorità di controllo e l'eventuale pagamento di danni può essere richiesto in qualsiasi sede giudiziaria del danneggiato.


OMBRE
LUCI

Cresciuta consapevolezza dell'importanza della protezione dei dati personali in tutte le attività siano esse pubbliche o private. Oggi qualsiasi titolare che voglia adottare sistemi, procedure, dispositivi, applicazioni etc., aventi un impatto su informazioni relative all'interessato è consapevole del fatto che ne deve prendere in considerazione i riflessi sotto il profilo normativo.

E' evidente, tuttavia, che il passaggio dalla consapevolezza alla effettiva «presa in carico» della questione, il che vuol dire eseguire una valutazione del rischio, responsabilizzare i fornitori nel rispetto dei principi privacy by design e privacy by default, sensibilizzare gli utilizzatori della piattaforma etc., deve ancora essere completato. Manca, ad oggi, un effettivo automatismo.

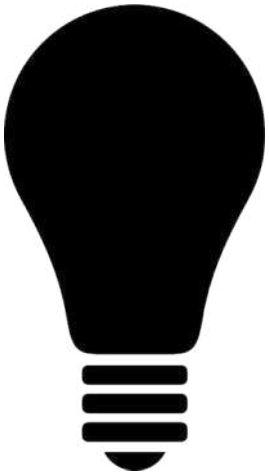
L’accresciuta importanza della materia relativa alla protezione dei dati personali può essere letta, anche, attraverso i numeri pubblicati dal Garante:

- 7.219 reclami, in aumento rispetto al 2018;
- 48.591 DPO/RPD;
- 946 notifiche di data breach;
- 18.557 contatti con l’Ufficio relazioni del Garante.

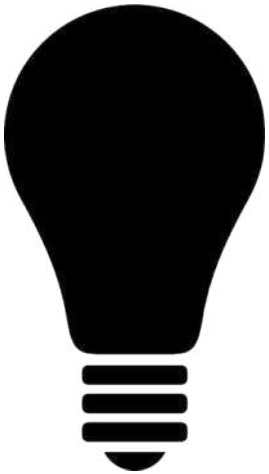
(Dati riferiti al periodo 25 maggio 2018 - 31 marzo 2019. Fonte: https://www.garanteprivacy.it/regolamentoue/bilancio)

Le principali azioni di implementazione delle aziende hanno riguardato:

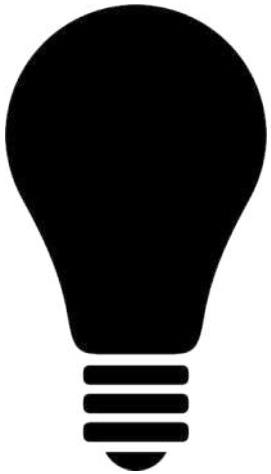
1. Creazione dei registri di trattamento;
2. Individuazione dei ruoli e delle responsabilità;
3. Raccolta e mappatura dei dati;
4. Modifica della modulistica e della contrattualistica: ad esempio, informative agli interessati, designazione dei responsabili, etc.;
5. Procedura di *data breach notification*;
6. Definizione delle politiche di sicurezza e valutazione del rischio;
7. Valutazione d'impatto sulla protezione dei dati personali;
8. Implementazione dei processi per l'esercizio dei diritti degli interessati.



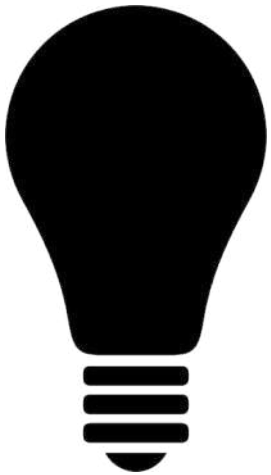
L’atteggiamento che molti titolari, sia privati che pubblici, hanno adottato, e molti continuano ancora a farlo, è stato quello di **approcciarsi al GDPR come se fosse ancora la normativa nazionale**, applicando gli stessi schemi formali che hanno contraddistinto la vecchia normativa.



Ancora oggi, ad un anno dall'applicazione, ci si rifugia nei **tecnicismi formali** (se nominare o meno il responsabile interno del trattamento, se continuare utilizzare il termine «incaricato» piuttosto che «autorizzato», oppure considerare il consenso privacy quale condizione sufficiente per trattare i dati personali dell'interessato).



Il DPO/RPD, figura nuova ed importante, ad oggi, salvo casi particolari, viene visto con un **approccio burocratico**, con il rischio di vivere un **isolamento** all'interno dell'organizzazione e subendo in alcuni casi delle vere e proprie frustrazioni.



Sempre in tema di DPO/RPD, le maggiori criticità hanno riguardato:

- Scelta del DPO/RPD basata sul criterio del minor costo (ad esempio poche centinaia di euro al mese, se non addirittura mille per un intero anno) e con incarichi limitati ad un anno;
- Validazione delle competenze specialistiche basate su attestazioni di frequenza a corsi di dubbia valenza specializzante: dei moderni *azzeccagarbugli* insomma;
- DPO/RPD che prestano la propria assistenza esclusivamente «on-line» e «a distanza»;
- DPO/RPD chiamati ad adottare in prima persona le «misure» di adeguamento al GDPR (adempimenti che il Regolamento invece riserva alla competenza esclusiva del titolare).

Tali criticità (ombre) sono state dettate da due fattori:

1. Non esiste cultura al recepimento in Italia; la cultura della privacy non riesce a germogliare (ne è un esempio il recentissimo furto di dati relativi ad oltre 30.000 avvocati e praticanti romani ad opera di un gruppo di hacker); Paura del nuovo, paura del cambiamento.

2. Difficoltà di declinare operativamente i principi del GDPR. Ad esempio, come si applicano in concreto i principi *privacy by design* e *by default* nei confronti degli stakeholder, oppure come eseguire una valutazione del rischio.

ASSINDUSTRIA VENETOCENTRO
IMPRENDITORI PADOVA TREVISO

UNIS&F

GRAZIE PER L'ATTENZIONE