Il data manager: la vera necessità del GDPR

L’interpretazione del testo di una norma è un processo complicato e che, per molti versi, deve snodarsi con fluidità nel tempo: il diritto vivente, direbbero i giuristi. Per me, che giurista non sono e che ho una passione per la statistica, esiste un modo artigianale per capire dove “mira” la legge: faccio una graduatoria, con l’aiuto di uno specifico software di analisi automatica del testo, delle parole più frequenti (opportunamente lemmatizzate). Naturalmente, uso questa tecnica nello step iniziale di approccio ai testi normativi di nuova emanazione. È un modo per capire su quali temi il legislatore ha voluto porre l’accento.

L’ho applicata, inizialmente, anche al Regolamento Europeo per la Protezione dei Dati Personali (GDPR). La classifica che è emersa è la seguente

Parola	Frequenza
trattamento	1363
Dato	883
personale	622
articolo	609
autorità	598
titolare	480
diritto	474
di controllo	462
interessare	421
membro	365

Le parole più presenti sono *trattamento* e *dato*. Sono questi i principali temi del GDPR. Stupisce che non ci siano, almeno tra le prime dieci, le parole *protezione* (15° posto) o

sicurezza (82° posto) o *finalità* (23° posto): il focus è sulle modalità di trattamento dei dati (*personali*, 3° lemma) nelle organizzazioni.

E questo mi ha sollecitato una riflessione: quante aziende o organismi pubblici si sono concentrati molto sugli obblighi esplicitamente previsti dal GDPR (DPIA, DPO, registri, misure di sicurezza, ecc.) e molto meno sul ciclo di vita del dato al loro interno?

Perché il dato è centrale

Siamo nell'era dei big data e, quindi, appare superfluo ribadire l'importanza del dato nella creazione del valore di una qualsiasi organizzazione (pubblica o privata). Ma il GDPR penetra più in profondità: la creazione del valore, che non è negata ma apprezzata (Considerando n. 10), deve accompagnarsi alla tutela dei *diritti* (parola che ha meritato il 7° posto) e delle libertà delle persone e basarsi su alcuni principi (riferiti appunto ai dati ed ai trattamenti) funzionali a garantirli.

I principi stabiliti dal GDPR hanno, quindi, una relazione *diretta* con il dato oppure *mediata* quando sembrano riferirsi alle operazioni di trattamento. Questo è il motivo per cui il dato è centrale e richiede che sia costantemente curato rispetto a

- liceità, cioè esistenza di una base giuridica per poterlo trattare;
- correttezza, cioè assenza di comportamenti potenzialmente lesivi nei confronti dell'interessato;
- trasparenza, cioè garanzia dell'esercizio del controllo (inteso come una via di mezzo dei verbi inglesi *to check* e *to manage*) da parte dell'interessato;
- minimizzazione, cioè utilizzo solo e soltanto se indispensabile per le finalità previste;
- limitazione della conservazione, cioè utilizzo solo per

il tempo necessario al raggiungimento delle finalità previste;
- esattezza, cioè aderenza alla realtà del momento al quale si riferisce;
- sicurezza, cioè disponibilità, integrità e riservatezza.

Questi sono i principi, previsti dall'art. 5 del GDPR, che costituiscono la base sulla quale edificare il modello di ciclo di vita del dato all'interno di ogni organizzazione.

Il data manager

Considerata la centralità del dato, una figura necessaria all'interno di ogni organizzazione è il data manager cioè il professionista attraverso il quale ogni organizzazione applica i principi di *privacy by design* e *privacy by default*, previsti dal GDPR. È l'esperto al quale è affidata l'ordinaria amministrazione dell'elemento più importante: il dato.

Gli obiettivi che sono affidati al data manager sono duplici:

- garantire che il ciclo di vita del dato sia effettuato secondo criteri di qualità e, conseguentemente, conformi alle previsioni di normative cogenti e di standard internazionali;
- garantire che l'organizzazione sappia rispondere ai diritti degli stessi interessati e, di conseguenza, sappia tutelarli, evitando di incorrere nelle sanzioni previste dal GDPR.

Molte organizzazioni si sono, doverosamente, affrettate ad individuare il Data Protection Officer, il responsabile del trattamento ed a capire quali erano i nuovi adempimenti per essere conformi al GDPR. Ma è sufficiente? La sostenibilità nel tempo della compliance al GDPR passa, soprattutto, dalla presenza del data manager e dalla sua esatta collocazione all'interno dell'organizzazione e dal suo rapporto con le altre figure (siano esse obbligatorie o facoltative).

Per questo è importante spiegare quali sono i tratti distintivi del data manager e delinearne le attività specifiche.

Data manager vs DPO

Il data manager è una figura diversa dal Data Protection Officer per le seguenti ragioni:

- è una figura che fa parte integrante dell'organizzazione e partecipa alle decisioni che riguardano le finalità e le modalità di trattamento;
- non ha il compito di sorvegliare l'osservanza del GDPR ma si occupa di curare il ciclo di vita del dato;
- non ha, quale attività specifica, la cooperazione con l'autorità di controllo;
- non ha, di norma, contatti diretti con gli interessati.

La diversità dei ruoli non esclude che data manager e DPO, insieme alle altre figure aziendali, siano in frequente contatto per assicurare un approccio olistico alla protezione dei dati personali. Un punto di contatto di particolare rilevanza tra le due figure è, per esempio, l'attuazione delle procedure di prevenzione e di gestione dei data breach.

Data manager vs IT Manager

Il data manager è una figura diversa dall'IT Manager. Infatti, l'IT Manager si occupa di pianificare e gestire l'infrastruttura tecnologica di supporto ai processi aziendali. Il focus del data manager è, invece, sui dati e deve considerare le soluzioni tecnologiche adottate come un assioma del suo quadro di riferimento.

Anche in questo caso, è auspicabile che data manager e IT Manager, essendo peraltro due figure interne all'organizzazione, operino in stretta sinergia per ottimizzare le soluzioni tecnologiche finalizzandole al

massimo livello di protezione dei dati personali.

Data manager vs responsabile del trattamento

Il responsabile del trattamento è, per uniforme interpretazione dottrinaria del GDPR, un soggetto esterno all'organizzazione che esegue *in concreto* il trattamento dei dati personali. Il data manager, viceversa, opera all'interno dell'organizzazione e contribuisce, eventualmente, a fornire al responsabile del trattamento le istruzioni documentate richieste dall'articolo 28 del Regolamento.

In realtà, il data manager è cruciale anche nella scelta del responsabile del trattamento oltre che nella materiale redazione del contratto (o altro atto giuridico) previsto dal comma 3 dello stesso articolo 28. Infatti, il contratto integrerà certamente un Service Level Agreement basato su specifici indicatori riguardanti i dati e le loro caratteristiche.

Data manager vs privacy manager

Il data manager non effettua alcuna valutazione del rischio ed opera, di norma, a valle del lavoro svolto dal privacy manager. Un esempio classico che fa emergere la differenza dei ruoli è la decisione di applicare, dopo un definito periodo temporale, un processo di anonimizzazione dei dati dei clienti. La decisione di applicare una misura di sicurezza basata sull'anonimizzazione è del privacy manager che la individua dopo un'attenta valutazione dei rischi; il data manager, invece, deve definire le procedure per applicarla in maniera sistematica (alle scadenze temporali fissate) e completa (per l'intero database ed in modo che non sia possibile, in alcun modo, risalire all'identità dell'interessato).

Le specifiche attività del Data Manager

L’attività specifica del data manager è quella di assicurare un ciclo di vita del dato rispettoso:

- dei diritti degli interessati;
- delle policy stabilite dall’organizzazione;
- degli standard di qualità internazionali.

Questi tre goal sono tra loro inscindibili e richiedono, come prerequisito trasversale, la perfetta conoscenza della mappa completa dei dati trattati dall’organizzazione. Non si parla di mappa fisica (che è una specifica conoscenza dell’IT manager) ma di mappa logica e di flussi innescati dai processi di trattamento.

Nel lavoro del data manager assumono particolare rilievo gli standard ISO/IEC 25012:2014 “Modello di qualità dei dati” e ISO/IEC 25024:2015 “Misurazione della qualità dei dati”. Il primo è funzionale alla definizione delle caratteristiche che devono assumere i dati e, in qualche modo, di ausilio alla *privacy by design* mentre il secondo è maggiormente orientato alla verifica ordinaria della qualità del dato, anche attraverso attività di audit, e porta a convergere verso la *privacy by default*.

Com’è noto, lo standard ISO/IEC 25012:2014 suddivide le caratteristiche di qualità in *inerenti*, *dipendenti dal sistema* e *inerenti e dipendenti dal sistema*. Nella tabella che segue si delinea un’ipotesi di percorso logico che mostra quali sono le relazioni tra le caratteristiche di qualità e le operazioni di trattamento, passando attraverso i princìpi stabiliti del GDPR.

Tipi di caratteristiche di qualità	**Caratteristiche di qualità**	**Princìpi del GDPR**	**Operazioni di trattamento**

Inerenti	Accuratezza	Trasparenza Esattezza Integrità	Raccolta – Registrazione– Aggiornamento –Raffronto
	Attualità	Correttezza Trasparenza Esattezza Limitazione della conservazione	Raccolta – Registrazione Conservazione – Aggiornamento – Estrazione – Consultazione Limitazione – Cancellazione – Distruzione
	Completezza	Liceità Correttezza Trasparenza Minimizzazione Esattezza Integrità	Raccolta – Registrazione – Organizzazione – Conservazione – Aggiornamento – Estrazione
	Credibilità	Liceità Correttezza Trasparenza Esattezza	Aggiornamento – Estrazione – Consultazione– Raffronto

Inerenti e dipendenti dal sistema	Accessibilità	Correttezza Trasparenza	Organizzazione – Conservazione –Uso
	Comprensibilità	Trasparenza	Organizzazione –Consultazione – Uso –Raffronto
	Conformità	Correttezza Trasparenza	Raccolta – Registrazione – Organizzazione – Conservazione –Cancellazione – Distruzione
	Precisione	Correttezza Esattezza	Raccolta – Registrazione Aggiornamento –Consultazione – Uso – Comunicazione – Diffusione – Raffronto
	Riservatezza	Sicurezza	Registrazione – Organizzazione – Conservazione –Consultazione – Uso – Comunicazione – Diffusione – Limitazione – Cancellazione – Distruzione
	Tracciabilità	Sicurezza	Organizzazione – Conservazione –Estrazione – Consultazione – Uso – Comunicazione – Diffusione

Dipendenti dal sistema	Disponibilità	Correttezza Trasparenza Sicurezza	Organizzazione – Conservazione – Aggiornamento –Consultazione – Uso –Limitazione – Cancellazione – Distruzione
	Portabilità	Correttezza	Organizzazione – Conservazione –Comunicazione – Diffusione
	Ripristinabilità	Correttezza Trasparenza Sicurezza	Conservazione –Cancellazione – Distruzione

L'attenzione al percorso logico che conduce a governare opportunamente le operazioni di trattamento per garantire le caratteristiche di qualità e la protezione dei dati personali deve avere, come effetto indotto, la generazione di procedure specifiche per rispondere efficacemente alle richieste di esercizio dei diritti da parte dell'interessato. L'esempio più evidente è fornito dalla caratteristica di qualità che lo standard ISO/IEC 25012:2014 denomina *portabilità* e che, molto spesso, è trascurata nell'ambito delle organizzazioni; il GDPR eleva questa caratteristica di qualità ad un diritto specifico (art. 20 del GDPR) obbligando a considerarla cogente in sede di progettazione (by design) ed in sede di esercizio (by default) oltre che a definire procedure dirette a renderla effettiva nei termini previsti dal regolamento e richiesti dall'interessato.

Lo standard ISO/IEC 25024:2015 può essere d'ausilio al data manager per la definizione di procedure di audit sui dati. Infatti, vale sempre il vecchio motto di Kaplan "Non si può gestire ciò che non si può misurare". Quindi, partendo dalle misure previste dallo standard, il data manager può agevolmente individuare quelle più idonee ad assicurare il

mantenimento nel tempo delle caratteristiche di qualità nonché le procedure di auditing per la verifica delle stesse.

Conclusioni

Non bisogna dimenticare che il GDPR prevede, all'art. 5, un ulteriore principio: il principio di responsabilizzazione. Il titolare del trattamento dei dati personali è competente (traduzione dall'inglese *responsible*) per il rispetto degli altri principi previsti dallo stesso articolo e deve essere in grado di comprovarlo. Il modo migliore per rispettare questo principio, soprattutto per le grandi organizzazioni, è quello di individuare un professionista specifico per curare il ciclo di vitta del dato: il data manager, appunto.

A cura di: **Francesco Maldera**



Francesco Maldera è Data Protection Officer e Data Scientist.

Il suo percorso professionale lo ha chiamato a responsabilità direzionali nell'ambito dei sistemi informativi, della safety&security, della privacy e dell'auditing svolgendo diversi incarichi dirigenziali nella Pubblica Amministrazione e in aziende private.

Attualmente, accompagna l'attività consulenziale a quella di sensibilizzazione delle persone tramite il sito www.prontoprivacy.it



https://www.ictsecuritymagazine.com/articoli/il-data-manager-la-vera-necessita-del-gdpr/