Oracle Community For Security

GDPR:
Maturità delle Imprese italiane rispetto agli adempimenti richiesti

Survey 2018

protiviti®
Face the Future with Confidence

ORACLE®

Executive Summary

L'attuazione da parte delle aziende del Regolamento 2016/679, noto anche come GDPR ("*General Data Protection Regulation*"), che ha rivoluzionato completamente il precedente impianto normativo in materia di protezione dei dati personali, determinando un radicale cambio di prospettiva rispetto al passato, deve essere vista non solo come un costo, ma anche come un'opportunità per migliorare l'efficacia dei processi di business e per lo sviluppo del proprio mercato. Basti pensare alle aziende che operano a stretto contatto con il consumatore: la consapevolezza dei clienti che i dati personali loro riferiti siano protetti in maniera adeguata permetterebbe di incrementare il rapporto di fiducia nei confronti delle singole imprese, aumentando al contempo i vantaggi in termini di business.

Questa è la chiave di lettura che deve guidare le singole organizzazioni nel mettere in atto gli adempimenti che la nuova normativa impone.

Il considerando n. 1 del GDPR recita: *"La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale*". Ne deriva che le aziende devono attuare misure che garantiscano ai cittadini un miglior controllo dei propri dati e assicurino che questi ultimi siano adeguatamente tutelati nell'era del digitale, dell'IoT e del continuo sviluppo di nuove tecnologie.

La *survey*, condotta da Oracle Community for Security e realizzata nel periodo compreso tra marzo e giugno 2018, ha permesso di rilevare il generale grado di maturità delle imprese rispetto agli adempimenti richiesti dal nuovo Regolamento, identificando quelli sui quali ci sia un buon livello di adeguamento e quelli che, invece, richiedono ancora sforzi importanti. È importante agire subito: il periodo di transizione posto dal legislatore europeo per adeguarsi al nuovo Regolamento è terminato e le sanzioni dallo stesso previste sono divenute, a tutti gli effetti, applicabili.

Introduzione

Il nuovo Regolamento Europeo in materia di protezione dei dati personali, pubblicato sulla Gazzetta Ufficiale dell'UE lo scorso 4 maggio 2016 è diventato definitivamente applicabile a partire dal 25 maggio 2018. Come noto, introduce novità di fondamentale rilievo, che impongono di rivedere i modelli di gestione della privacy adottati dalle aziende. Ciò vale, in particolare, per:

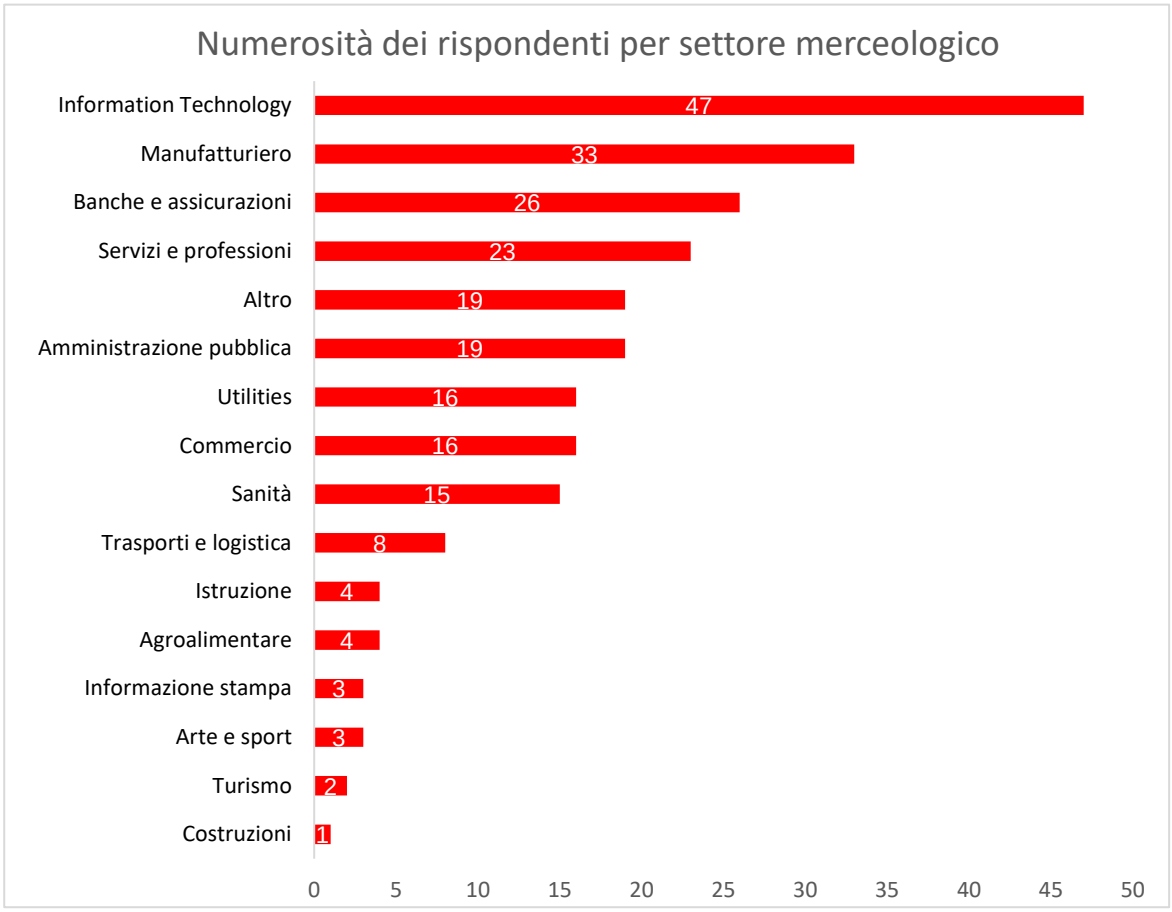
- Il principio di accountability ("responsabilizzazione" nella traduzione italiana), il quale impone al Titolare di adottare comportamenti proattivi ed essere in grado di dimostrare che i trattamenti vengano effettuati in conformità al GDPR mediante l'adozione, tra le altre cose, di adeguate misure tecniche ed organizzative;
- Il registro delle attività di trattamento, che deve contenere almeno gli elementi prescritti in via obbligatoria dall'art. 30;
- La figura del Responsabile della Protezione dei Dati (DPO, ovvero "*Data Protection Officer*"), da nominare obbligatoriamente nelle ipotesi individuate dall'art. 37;
- L'obbligo di modificare la documentazione privacy finora utilizzata (informative, moduli di raccolta del consenso, lettere di nomina a responsabile del trattamento), tenendo conto degli elementi di novità previsti al riguardo dagli artt. 13, 14 e 28 del GDPR;
- L'esigenza di predisporre policy e/o procedure che consentano di mettere in atto i nuovi adempimenti previsti dal GDPR, tra cui:
  - L'adozione di adeguate misure tecniche ed organizzative fin dall'inizio delle operazioni di trattamento di dati personali (*privacy by design*);
  - La notifica di eventuali violazioni di dati personali al Garante Privacy e l'eventuale comunicazione delle stesse anche agli interessati (*data breach*);
  - La valutazione dell'impatto di operazioni di trattamento di dati personali che presentino un rischio elevato per i diritti e le libertà delle persone fisiche (valutazione d'impatto sulla protezione dei dati);
  - La necessità di rivedere i contratti con i fornitori che trattino dati personali per conto del Titolare del trattamento, disciplinando adeguatamente gli aspetti relativi alla protezione dei dati.

Le 239 aziende prese in esame attraverso la *survey* appartengono a settori merceologici tra loro differenti e ciò ha consentito di avere una visione sul livello di *compliance* che fosse relativa a ciascuno degli ambiti in cui le stesse si trovano ad operare.

Come evidenziato nel grafico che segue, la maggior parte dei rispondenti opera negli ambiti dell'*Information Technology*, *Manifatturiero, Bancario* e *Finanziario*, *Utilities*, *Servizi e Professioni*. Ad ogni modo, seppure in maniera ridotta, sono stati presi in esame anche altri settori, quali ad esempio quello della *Sanità* e del *Commercio*.

In particolare, il settore dell'IT è quello con il maggior grado di maturità rispetto agli adempimenti previsti dal GDPR, verosimilmente in ragione del forte impatto che le previsioni del nuovo Regolamento hanno su tale settore merceologico (basti pensare, ad esempio, ai principi di *privacy by design* e *by default*, o alla necessità di adottare misure di sicurezza adeguate ai rischi per i diritti e le libertà degli interessati). Inoltre, la preesistenza di un'ampia regolamentazione di settore in

alcuni ambiti (in particolare, in quello Bancario) ha senza dubbio fornito un valido supporto per l'adeguamento alle nuove disposizioni contenute nel GDPR.



Fonte: Oracle Community For Security

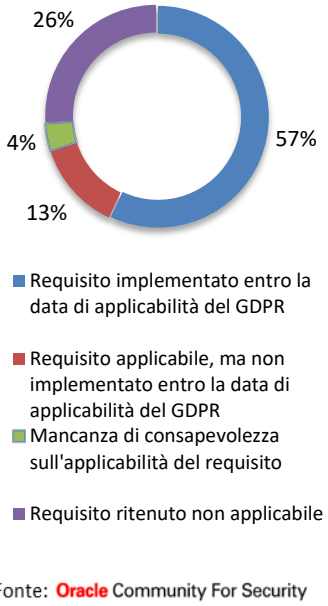
Ambiti di indagine e Risultati

Ciò premesso, nel prosieguo forniamo un'analisi di quanto emerso rispetto ai diversi ambiti di indagine coperti dal questionario.

1) Responsabile della protezione dei dati ("Data Protection Officer")

Una delle domande presentate all'interno della *survey* riguarda la figura del Data Protection Officer (DPO), che rappresenta una delle principali novità introdotte dal GDPR, regolamentata agli artt. 37 e s.s. dello stesso.

Assegnazione del ruolo di DPO



Fonte: Oracle Community For Security

In particolare, è stato richiesto alle aziende partecipanti se all'interno della loro struttura fosse stato o meno assegnato questo ruolo. Più della metà dei rispondenti, pari al **57%** del totale (di cui il **10%** appartenente alle aziende operanti nel settore dell'*Information Technology*) ha confermato di aver effettuato tale nomina.

Il **13%** delle aziende partecipanti ha invece confermato di non aver adempiuto al requisito dalla nomina prima della definitiva applicabilità del Regolamento.

Questo valore è rappresentato per la maggior parte dai settori del Commercio, della Sanità, dell'Amministrazione Pubblica e del Manifatturiero, con una percentuale prossima al **2%** ognuno.

Il rimanente **30%**, invece, è così ripartito: il **26%** appartiene alle imprese nelle quali la nomina di questa figura non risulta applicabile in base al GDPR, mentre il rimanente **4%** fa riferimento ai rispondenti che non sanno se all'interno della propria organizzazione tale figura sia stata o meno introdotta.

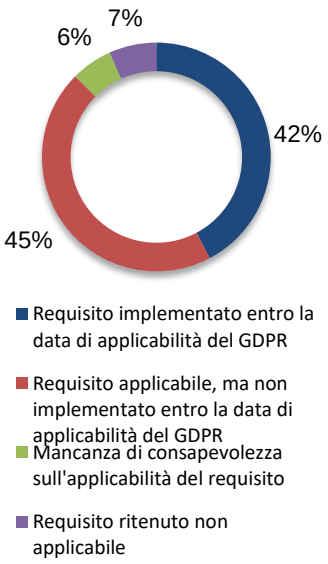
L'introduzione della figura del DPO è consigliabile anche per quelle aziende che non rientrerebbero nelle ipotesi di nomina obbligatoria previste dal GDPR. Le aziende, infatti, dovrebbero istituire un modello organizzativo che contempli tale soggetto quale figura incaricata a garantire il governo e il monitoraggio della *privacy* all'interno dell'organizzazione.

Ad ogni modo, sia nel caso in cui il DPO debba essere nominato obbligatoriamente, sia nel caso in cui ciò sia rimesso alla discrezionalità della singola azienda, esso dovrà necessariamente rispettare i requisiti previsti dal GDPR, tra cui quelli di indipendenza e assenza di conflitti di interesse nell'esecuzione delle proprie attività. Ne deriva che, qualora si opti per la nomina di un DPO interno, dovrà essere individuata l'area aziendale che meglio garantisca il rispetto di tali requisiti, quali - ad esempio - le funzioni Legal, Compliance o eventualmente una funzione *ad hoc*.

2) Contratti di fornitura

Un altro ambito sottoposto ai partecipanti riguarda l'aggiornamento/revisione di contratti con fornitori che trattano dati personali per conto del Titolare nello svolgimento di determinati servizi.

Revisione dei contratti di fornitura



Fonte: Oracle Community For Security

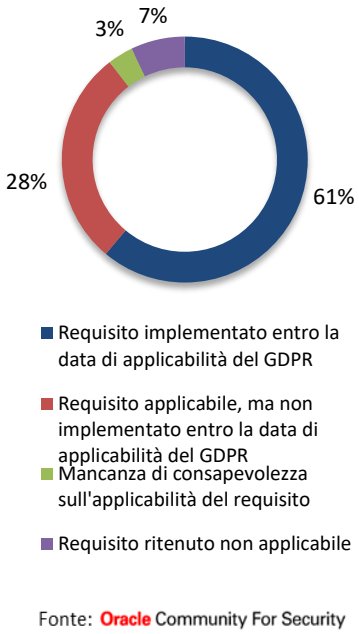
Questo è il tema che presenta risposte con le percentuali più bilanciate, con circa il 42% di aziende che hanno già provveduto all'aggiornamento/revisione dei contratti, a fronte di una percentuale, pari al 45%, che non ha ancora provveduto ad effettuare tale adempimento. A conferma di quanto affermato in precedenza, il settore che presenta la percentuale maggiore, considerando entrambi gli esiti, è quello relativo all'Information Technology, con un valore pari a circa il 12% di risposte positive.

A questo riguardo, data la numerosità dei contratti da analizzare e - potenzialmente - rivedere, si evidenzia come sia utile in primo luogo effettuare una mappatura dei fornitori e definire un piano di intervento, valutando in sostanza quali tra questi risultino particolarmente "critici", in quanto trattano una gran quantità di dati per conto del Titolare e/o categorie particolari di dati personali.

3) Informative

Altro aspetto di particolare rilevanza è costituito dalla revisione dei modelli di informativa finora adottati per garantire il rispetto delle previsioni di cui agli artt. 13 e 14 del Regolamento.

Revisione delle informative agli interessati



Fonte: Oracle Community For Security

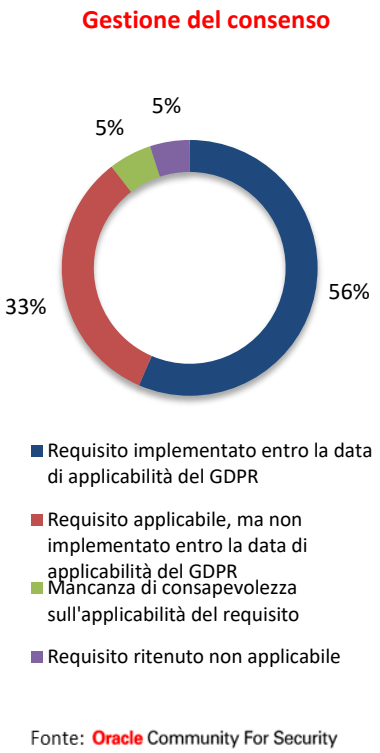
In particolare, è necessario aggiornare le informative in uso tenendo conto degli elementi di novità previsti a riguardo dal Regolamento, indicando - ad esempio - anche la base giuridica del trattamento, il periodo di *data retention* e i dati di contatto del DPO, se nominato.

In merito a questo aspetto, il **61%** dei partecipanti alla *survey* ha confermato di aver aggiornato le informative *privacy* con i nuovi riferimenti indicati nel Regolamento. Tra questi, è ancora il settore relativo all'*Information Technology* (con un valore pari a circa il **20%**) a presentare la percentuale maggiore di risposte affermative.

Il **28%** delle risposte è da associare, invece, alle aziende che hanno fornito una risposta negativa, di cui il **6%** appartiene al settore Manifatturiero, che risulta essere il più indietro nell'aggiornamento dei modelli di informativa da fornire agli interessati.

4) Consensi

Strettamente correlato alla revisione delle informative è il tema della corretta gestione dei consensi.



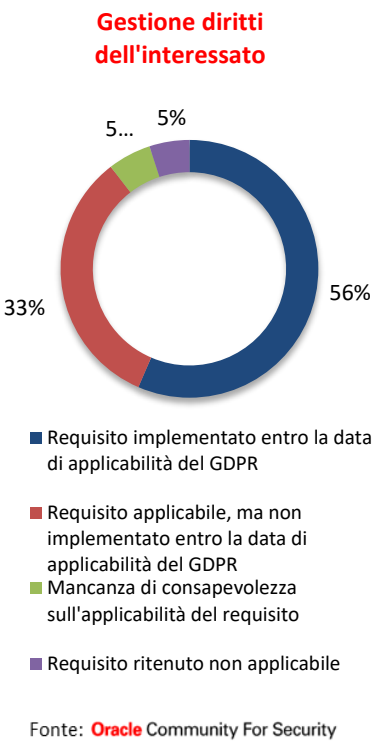
Ciascun Titolare, in particolare, deve implementare un sistema strutturato che consenta di tenere traccia dei consensi rilasciati nel tempo dagli interessati. Ciò al fine di garantire che, rispetto a quelle operazioni di trattamento la cui base giuridica sia costituita dal consenso, il Titolare possa essere in grado di dimostrare di averlo raccolto correttamente.

A tal proposito, più della metà delle aziende intervistate, con un valore del **56%** circa (**20%** per il solo settore dell'*Information Technology)*, ha precisato di raccogliere e utilizzare in modo accurato il consenso rilasciato dagli interessati. Il **33%** delle aziende intervistate, invece, non ha ancora provveduto a definire un modo strutturato di gestione del consenso.

I settori più arretrati, sotto questo punto di vista, sono il Manifatturiero e la Pubblica Amministrazione, che presentano, rispettivamente, risposte negative pari all'**8%** e al **5%** rispetto al campione complessivo.

5) Applicazioni e procedure per i diritti di accesso, oblio, portabilità

Ulteriore adempimento richiesto dalla nuova normativa è la definizione di procedure per la gestione dei diritti degli interessati, quali ad esempio i diritti di accesso, oblio e portabilità.



La definizione di tali procedure deve essere accompagnata dall'adozione di misure tecniche ed organizzative adeguate, volte a garantire che il Titolare del trattamento possa effettivamente fornire agli interessati un riscontro entro i termini previsti dalla nuova normativa (1 mese, estendibile fino a 2 mesi in casi di particolare complessità).

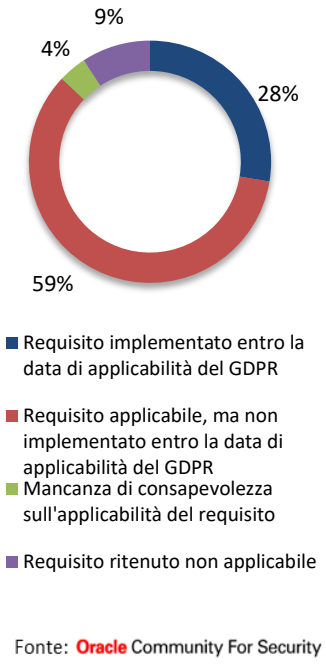
La maggior parte delle risposte a questo requisito sono negative, arrivando ad attestarsi al **56%** circa del totale dei partecipanti alla *survey*. Tra queste, i settori che presentano le percentuali più alte, pari rispettivamente al **9%** e **8%,** sono quelli del Manifatturiero e Bancario – Assicurativo.

Dai risultati si evince, invece, che solo il **30%** delle imprese rispondenti è in linea con le disposizioni previste dal Regolamento (la percentuale maggiore è rappresentata dal settore dell'*Information Technology,* con quasi il **9%** del totale).

6) Applicazioni e procedure per il rispetto dei criteri di minimizzazione e conservazione limitata nel tempo

In aggiunta alle procedure per l'esercizio dei diritti degli interessati, ne dovranno essere implementate altre che stabiliscano i principi per il trattamento dei dati personali all'interno della singola organizzazione, tenendo conto delle regole fissate al riguardo dal Regolamento, tra le quali quella secondo cui devono essere trattati soltanto i dati strettamente necessari in relazione alle finalità per le quali sono stati raccolti ("minimizzazione"), finalità da enunciare nell'informativa fornita agli interessati.

Criteri di minimizzazione e conservazione limitata nel tempo



Fonte: Oracle Community For Security

In secondo luogo, dovrà essere definita una policy di *data retention* che stabilisca il periodo di conservazione dei dati trattati all'interno dell'azienda, nel rispetto del principio secondo il quale i dati devono essere conservati per il tempo necessario al raggiungimento delle finalità per le quali sono trattati ("limitazione della conservazione").

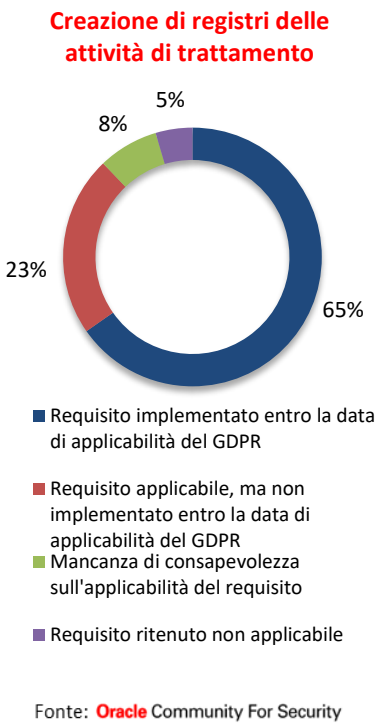
Ne deriva che anche le applicazioni e i sistemi devono essere progettati in maniera tale da garantire l'effettiva cancellazione dei dati raccolti allo scadere del termine fissato, oltre che la raccolta dei soli dati che risultino strettamente necessari (principio di *privacy by default*).

Tra tutti gli argomenti affrontati dai partecipanti alla *survey*, questo è quello che ha mostrato la percentuale più alta di risposte negative.

Infatti, circa il **60%** degli intervistati ha confermato di non essere ancora riuscito ad uniformarsi agli adempimenti richiesti dal Regolamento. Solo il settore dell'*Information Technology*, con circa l'**8%** di risposte positive, presenta la percentuale maggiore di risposte positive, con un valore pari al **30%** circa.

7) Registro delle attività di trattamento

Altra domanda somministrata ai partecipanti alla *survey* è relativa allo stato di implementazione del registro dei trattamenti di cui all'art. 30 del GDPR.



Al riguardo, occorre ricordare che, al di là delle ipotesi di obbligatorietà previste dal Regolamento, la tenuta del registro costituisce un adempimento consigliabile anche per le aziende che ne sarebbero esonerate, in quanto rappresenta uno strumento utile a mappare in maniera ordinata i trattamenti di dati personali effettuati all'interno della singola organizzazione e dimostrare la conformità ai principi del Regolamento.

Inoltre, sebbene il GDPR indichi il contenuto minimo che il registro dei trattamenti deve avere, sarebbe opportuno includervi anche informazioni ulteriori, quali ad esempio l'elenco degli applicativi utilizzati o la lista dei soggetti ai quali i dati vengono comunicati.

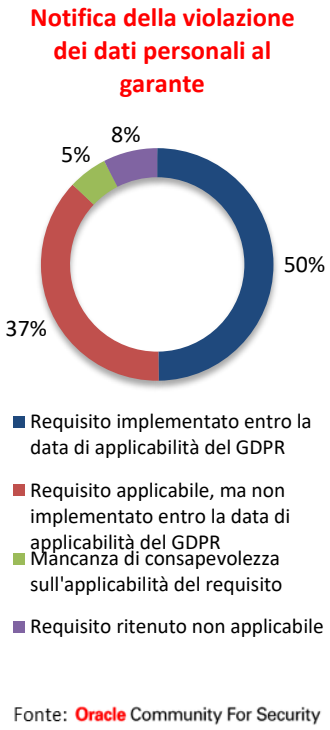
Infatti, ciò permetterebbe al Titolare del trattamento di gestire più agevolmente eventuali situazioni di *data breach*, oltre che di tenere traccia delle terze parti che devono essere nominate Responsabili del trattamento.

Tra tutti gli adempimenti richiesti dal nuovo Regolamento, questo ha riscosso la percentuale maggiore di risposte affermative: infatti, ben il **65%** delle aziende intervistate ha affermato di aver creato un registro delle attività di trattamento che presenta le informazioni elencate all'interno del già citato art. 30.

Le aziende che invece non hanno ancora provveduto a formalizzare un registro dei trattamenti, rispondendo in modo negativo alla specifica domanda, sono circa il **22%** del totale. In questo caso, a presentare la percentuale più alta di risposte negative, con un valore pari al **4%** circa, è il settore della Pubblica Amministrazione.

8) Procedure per la notifica di violazioni di dati personali al Garante Privacy e per la comunicazione agli interessati

La metà delle aziende partecipanti alla *survey*, con circa il **50%** di risposte positive, ha dimostrato di aver realizzato procedure per la notifica al Garante Privacy di violazioni di dati personali (c.d. *data breach*) e la comunicazione agli interessati.



Fonte: Oracle Community For Security

Il settore che presenta il maggior numero di risposte positive è quello relativo all'*Information Technology*, con circa il **10%** delle risposte totali.

Il **37%** delle imprese, invece, non ha ancora implementato tale requisito e il settore che presenta la percentuale maggiore di risposte negative è il Manifatturiero, con un valore superiore al **7%**.

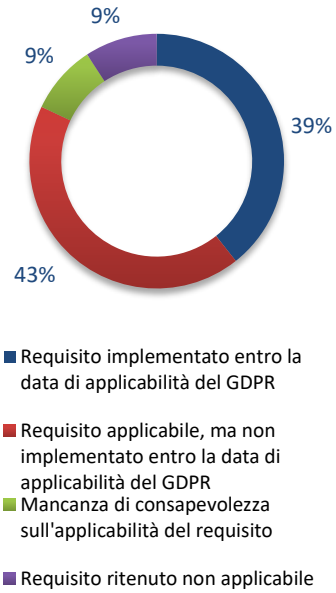
Questo è un aspetto che non deve in alcun modo essere trascurato.

Tale attività, infatti, deve essere accompagnata dalla capacità di determinare gli eventi che possano essere qualificati quali "*data breach*" e dall'individuazione dei soggetti all'interno di ciascuna azienda ai quali tali eventi debbano essere segnalati.

9) Misure di sicurezza

Da ultimo, è stato chiesto alle aziende partecipanti alla *survey* se avessero implementato delle misure di sicurezza aggiuntive rispetto a quelle previste dalla normativa previgente (ad esempio, quelle previste dall'Allegato B del D. Lgs. 196/2003).

Adozione misure di sicurezza aggiuntive



Fonte: Oracle Community For Security

Come noto, il GDPR non contiene più un elenco tassativo di misure da adottare, essendo rimessa al Titolare la definizione delle misure che possano ritenersi adeguate, tenendo conto dei rischi e delle finalità connesse alle operazioni di trattamento.

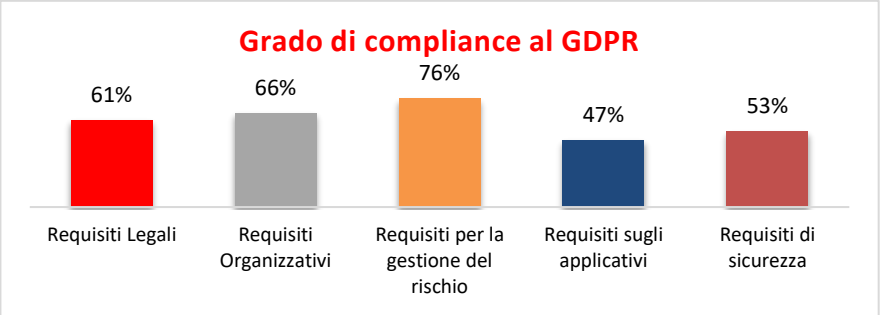
A titolo puramente esemplificativo, il GDPR indica quali misure di sicurezza la "pseudonimizzazione" e la cifratura dei dati personali, fermo restando che sarà onere del Titolare valutare caso per caso quali misure tutelino adeguatamente i dati personali oggetto di trattamento.

Al riguardo, il **43%** delle aziende intervistate ha affermato di non aver ancora posto in essere tali adempimenti.

L'unica eccezione riguarda il settore dell'*Information Technology*, il quale, con il **13%** circa di risposte positive, rappresenta un terzo delle risposte affermative complessive.

Ambiti di indagine e Risultati

La ricerca ha permesso, infine, di valutare il grado di compliance complessivo alle nuove previsioni del GDPR delle aziende rispondenti, suddividendo le domande nelle 5 classi indicate nel grafico seguente. A questo, si precisa che le percentuali sotto riportate sono state calcolate non considerando le risposte che indicavano "Mancanza di consapevolezza sull'applicabilità del requisito".



Fonte: Oracle Community For Security

A titolo di esempio, gli obblighi relativi alla nomina del DPO o alla revisione delle policy/procedure finora adottate all'interno dell'azienda sono stati inseriti nell'ambito della categoria dei "Requisiti Organizzativi"; quelli aventi ad oggetto la revisione dei contratti con i fornitori e delle informative fornite agli interessati sono stati fatti rientrare all'interno della categoria "Requisiti Legali".

Ebbene, da tale analisi emerge come gli ambiti rispetto ai quali le aziende mostrano un grado di maturità maggiore sono costituiti da quelli riguardanti la valutazione dei rischi e la definizione degli aspetti organizzativi e legali. Con riguardo a tale ultimo aspetto, in particolare, appare utile evidenziare come la definizione di modalità per la notifica di violazioni di dati personali all'Autorità Garante, la gestione dei diritti degli interessati, l'applicazione del principio data protection by design e by default debba essere parte di un processo strutturato, che preveda l'adozione di policy e procedure che descrivano nel dettaglio le modalità attraverso le quali tali adempimenti debbano essere effettuati.

Tali attività non possono essere realizzate in maniera occasionale, senza stabilire fin dall'inizio le regole da seguire al riguardo. Di converso, le due aree in maggiore sofferenza sono quelle relative ai requisiti sugli applicativi e alla sicurezza.

Rispetto ai primi, riteniamo che il ritardo sia dovuto alla complessità delle modifiche applicative richieste per garantire i diritti degli interessati (es. diritto all'oblio). Infatti, per procedere alla cancellazione dei dati personali dai sistemi informativi, bisogna avere contezza dei vincoli legali, della logica dell'applicazione e del modello dei dati del sistema.

Rispetto ai secondi - i requisiti di sicurezza - riteniamo che molte aziende debbano ancora istruire i progetti relativi a quest'area: cifratura dei dati e anonimizzazione in primis, ma anche controllo accessi, produzione, raccolta e analisi dei log e aggiornamento e messa in sicurezza (hardening e patching) dei sistemi hardware e software.

Conclusioni

La gestione della privacy è un tema che assume carattere trasversale, abbracciando ambiti tra loro diversi (legale, organizzativo, tecnologico, ecc.). Ne deriva che per garantire la piena compliance dell'azienda alle previsioni del GDPR occorre costruire un piano di adeguamento efficace, che copra i diversi aspetti che la nuova normativa introduce o regolamenta in maniera differente rispetto al passato.

È evidente che l'obbligo di porre in essere gli adempimenti previsti dal Regolamento rappresenta per le imprese l'occasione di migliorarsi e di diventare maggiormente competitive sul mercato, ad esempio aumentando la fiducia dei consumatori e diminuendo il rischio di eventuali perdite reputazionali, sebbene esso comporti senza dubbio la necessità di effettuare investimenti e di mettere a disposizione risorse.

Il GDPR determina un cambiamento epocale per quanto riguarda il tema della protezione dei dati personali, anche in ragione dell'introduzione del principio di accountability. Esso, d'altro canto, si accompagna alle recenti novità in via di introduzione ad opera della proposta di Regolamento E - Privacy, presentata il 10 gennaio 2017 e ancora non approvata in via definitiva. Quest'ultima, pur avendo numerosi punti di contatto con il GDPR, è centrata sul tema della protezione dei dati personali nello specifico settore delle Comunicazioni Elettroniche.

È evidente che i dati assumono un'importanza fondamentale nella nostra società: in ogni momento abbiamo a che fare con smartphone e altri dispositivi "intelligenti" connessi ad Internet, che producono dati su scala sempre crescente. Da qui la necessità di introdurre una regolamentazione uniforme a livello europeo, che nell'ottica del mercato unico digitale consenta di affrontare efficacemente le sfide dell'odierna e futura economia mondiale basata sui dati personali.

Le imprese, dal canto loro, dovrebbero sfruttare efficacemente questo momento, affinché si traduca in un vantaggio competitivo, di lungo periodo, per ognuna di esse.