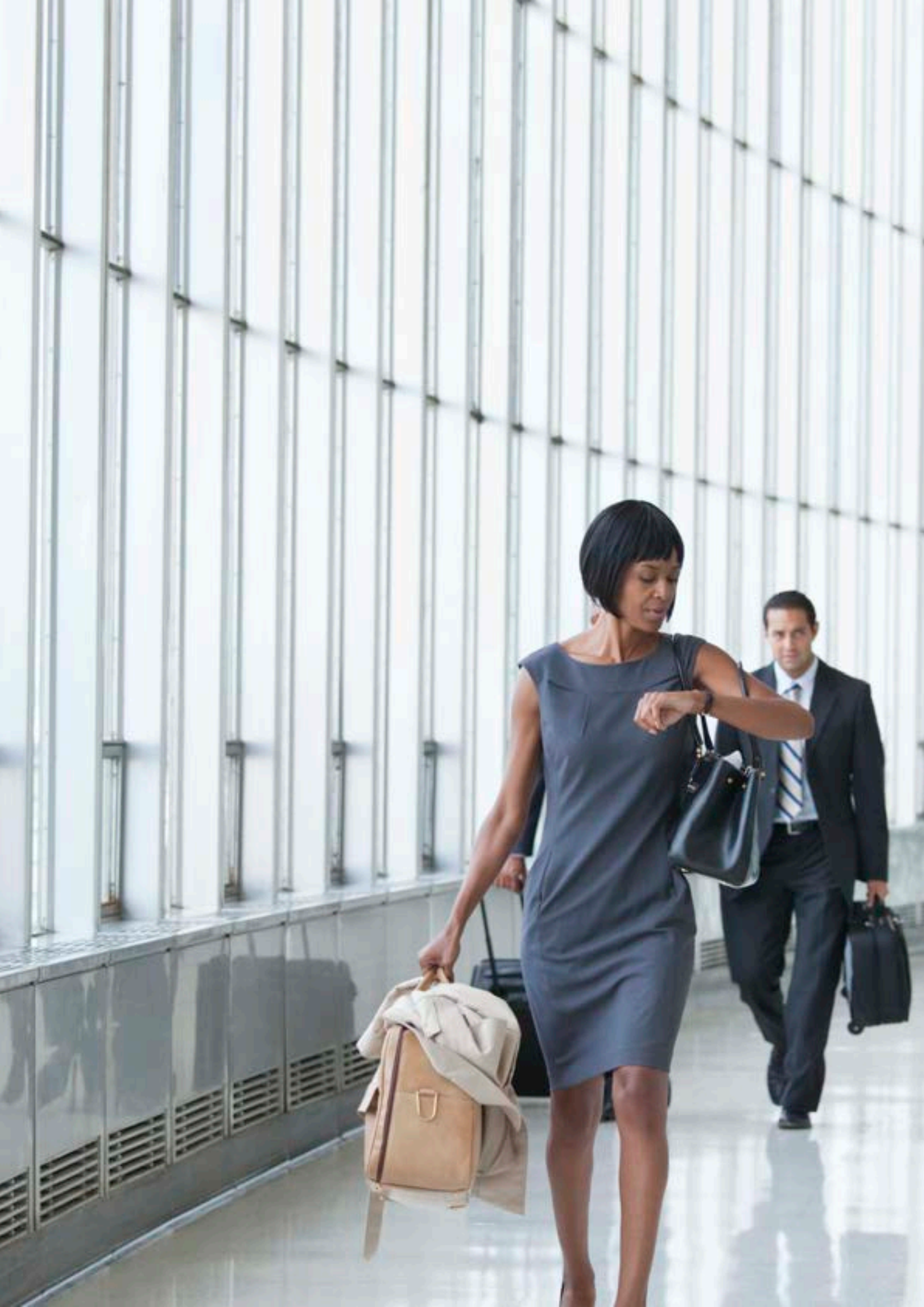
pwc

GDPR Maturity Survey

pwc.com/it



Contenuti

01 Introduzione

Al fine di disporre di informazioni utili sulle modalità o sulle caratteristiche di effettiva applicazione della normativa in ambito GDPR, PwC ha effettuato una *survey* attraverso la somministrazione di un questionario a Società/Gruppi operanti in settori differenti.

Numero totale dei rispondenti alla survey: 66

Il questionario, composto di **46 domande**, è stato inviato e raccolto nel **quarto trimestre 2019**.

I dati riportati nella presente *survey*, rappresentati in forma anonima, afferiscono esclusivamente alle Società/Gruppi che hanno risposto a tutte le domande del questionario.

Gli ambiti considerati nel questionario e rappresentati nel prosieguo del documento sono i seguenti:

- contesto generale;
- principi;
- diritti dell'interessato;
- ruoli e responsabilità;
- misure di sicurezza.

I rispondenti alla survey:

- sono stati raggruppati secondo la logica dell' indice di classificazione aziendale (ICB)*;
- sono stati suddivisi in 3 cluster in relazione ad un *privacy overall impact* attribuito in relazione al loro business.

Nel documento, per alcune tematiche soggette a interpretazione, sono state fornite indicazioni/definizioni ritenute utili per l'utilizzo di alcuni strumenti, funzionali al raggiungimento dei requisiti richiesti dal GDPR.

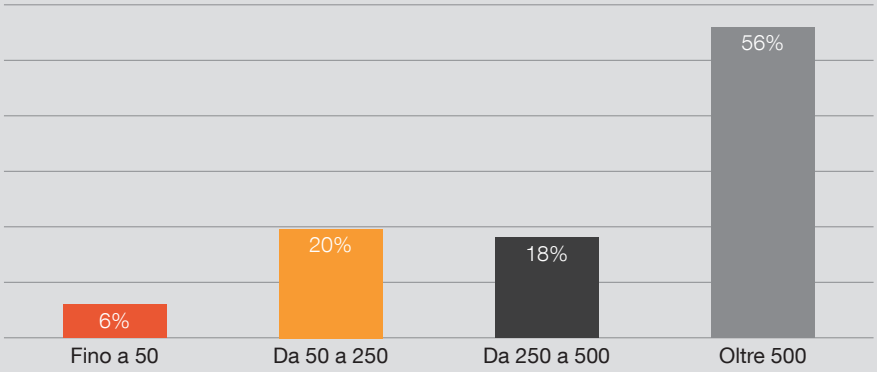
* L'Indice di classificazione industriale (ICB) è una tassonomia di classificazione industriale lanciata da Dow Jones e FTSE nel 2005 e ora utilizzata da FTSE International e STOXX. È utilizzato per separare i mercati in settori all'interno della macroeconomia.

02 Società & Settori

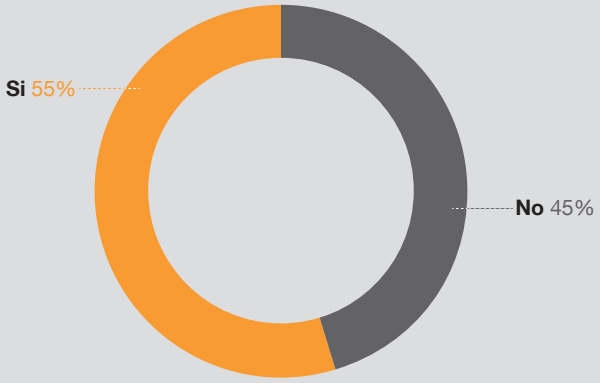
I rispondenti alla survey sono rappresentati attraverso la loro classificazione secondo le seguenti caratteristiche principali:

- n. dipendenti;
- fatturato dell'esercizio 2018;
- presenza di altre sedi in paesi UE;
- presenza sul mercato azionario.

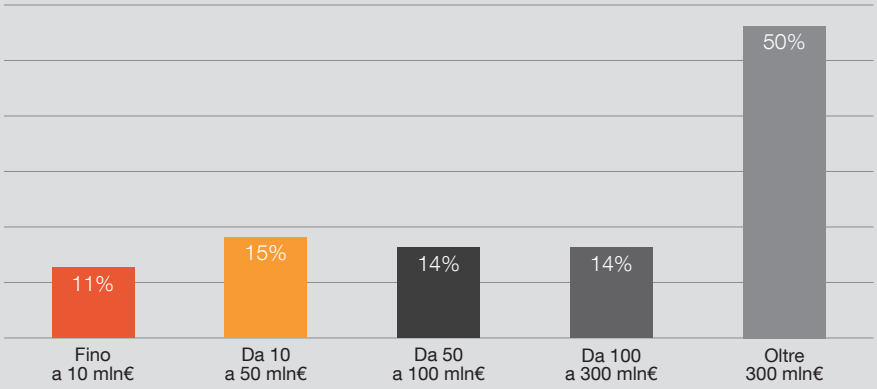
N° dipendenti impiegati nelle società rispondenti



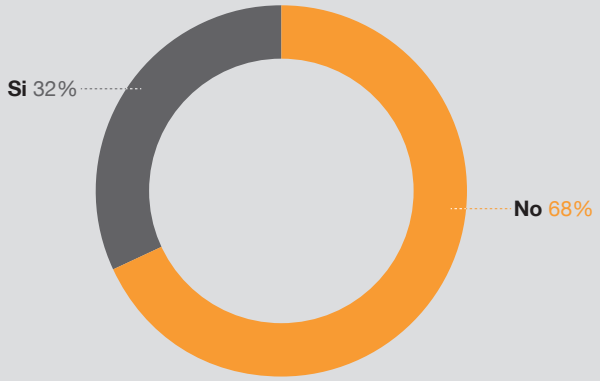
Presenza di altre sedi in paesi UE



Fatturato (riferimento all'esercizio 2018)

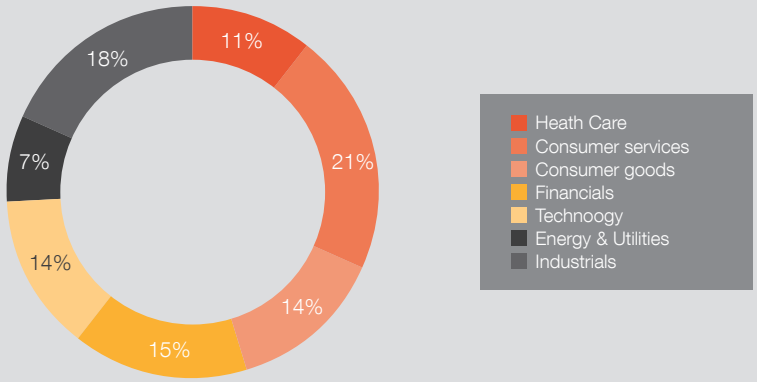


Presenza sul mercato azionario

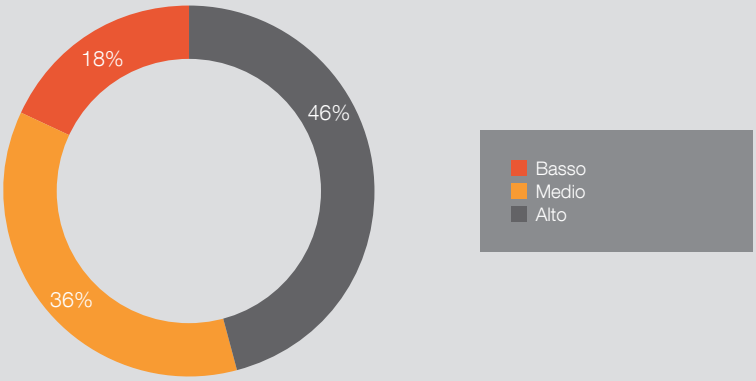


Settore di operatività & “Privacy overall impact classification”

Indice di classificazione aziendale



Privacy overall impact



Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

Le realtà rispondenti alla *survey*, precedentemente raggruppate secondo la logica dell’**ICB**, sono state suddivise in **3 *cluster*** in relazione ad un *privacy overall impact* («P.O.I.») attribuibile in relazione al loro *business*.

I **tre *cluster*** sono stati determinati, facendo riferimento:

- al numero di trattamenti che in media le aziende di un determinato settore ha definito;
- alla presenza sul mercato B2C.

03 Privacy: Contesto generale

Il **56%** delle aziende rispondenti alla survey dichiara di non avere ancora completato il progetto di adeguamento ai requisiti previsti dal GDPR.

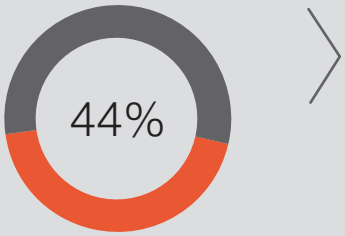
In particolare, alla data di compilazione della survey:

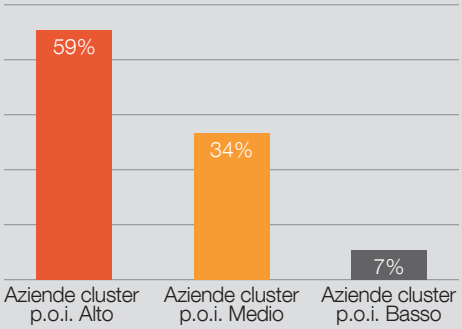
- il **20%** dichiara di stare ancora lavorando all'implementazione dei requisiti;
- il **36%** dichiara di stare lavorando all'adeguamento dei sistemi informatici.

Tutte le aziende rispondenti alla survey dichiarano di aver svolto l'attività di assessment iniziale.

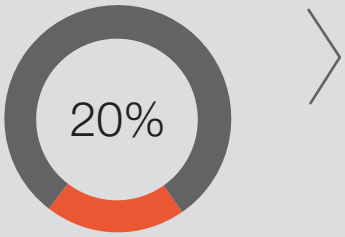
Il d.Lgs. 101/2018 prevedeva un "grace period" per l'attuazione soft del Regolamento e dal 20 maggio 2019 i requisiti del predetto d.Lgs. sono entrati a pieno regime. Qual è lo stato del progetto di adeguamento ai requisiti del GDPR?

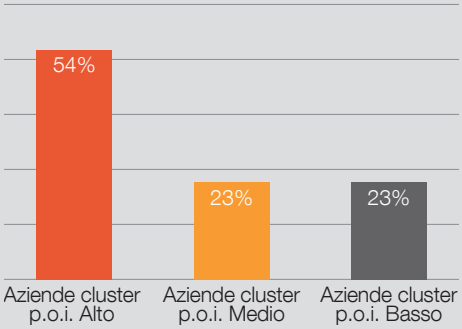
Le aziende dichiarano di aver completato il progetto di adeguamento ai requisiti del GDPR



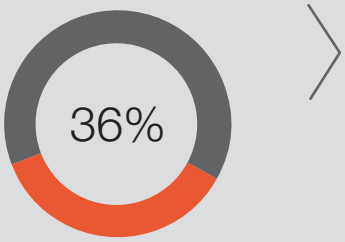


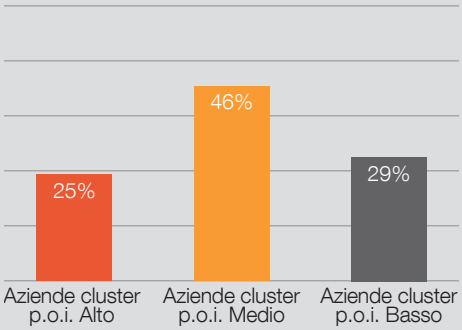
Le aziende dichiarano di aver effettuato una gap analysis e di star lavorando sull'implementazione dei requisiti





Le aziende dichiarano di aver adeguato i processi aziendali ai requisiti del GDPR ma di star lavorando sull'adeguamento dei sistemi informatici

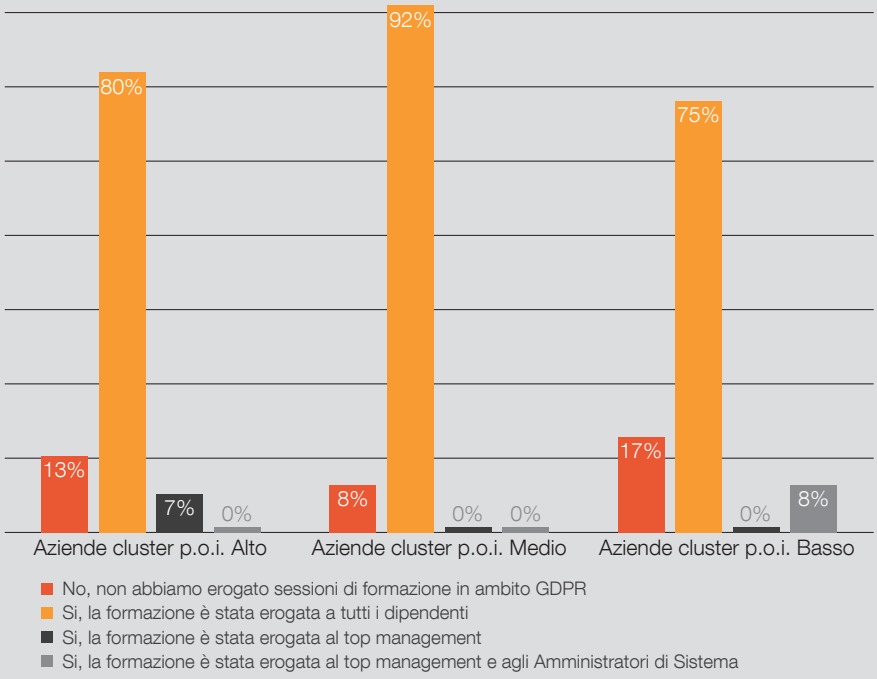




Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

A seguito dell'adeguamento ai requisiti introdotti dal GDPR, sono state svolte specifiche sessioni di formazione sui temi specifici del GDPR e di Data Protection?



Le aziende rispondenti alla survey dichiarano di aver svolto sessioni di formazione per tutti i dipendenti dell'organizzazione.

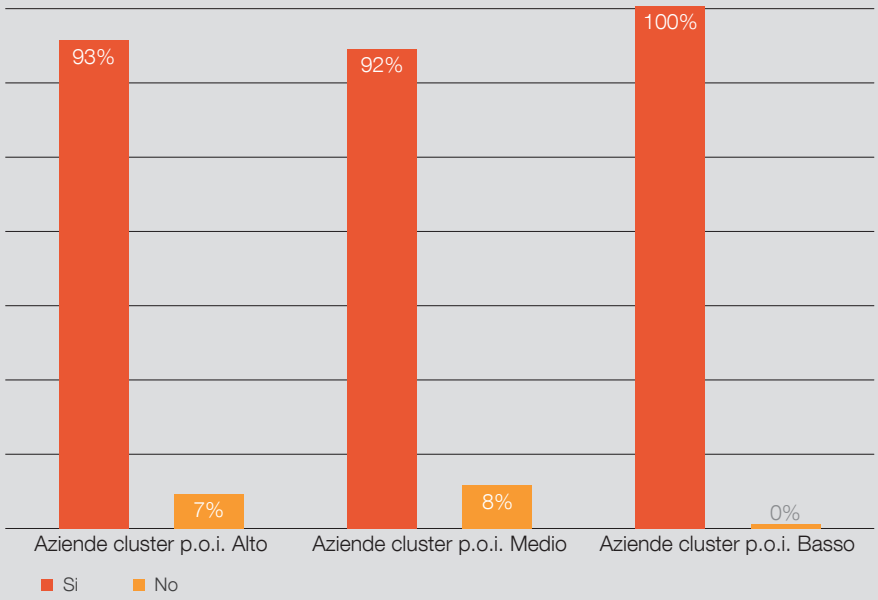
In media l'**80%** delle aziende rispondenti dichiara di aver formato tutto il personale dipendente sui nuovi requisiti introdotti dalla norma; assume valore superiore al 90% per le aziende classificate con privacy overall impact "medio".

Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

Il **94%** delle aziende rispondenti alla survey dichiara di aver eseguito un'attività di assessment finalizzata a comprendere se l'azienda trasferisce o meno i dati in paesi extra UE.

È stata eseguita un'attività di assessment volta ad identificare se vengono trasferiti dati in paesi extra UE?



Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

04 Principi

Il **100%** dei rispondenti alla *survey* dichiara di aver ritenuto opportuno regolamentare i principali aspetti di *Data Protection*. In particolare, i rispondenti dichiarano di aver definito procedure in ambito:

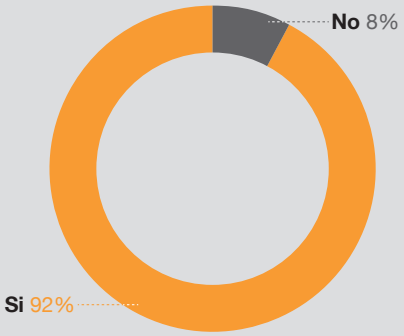
- *Data Breach;*
- Diritti di accesso;
- *Privacy by design/By default;*
- DPIA.

Circa il **17%** dei rispondenti dichiara di aver ritenuto opportuno redigere ulteriori procedure in ambito:

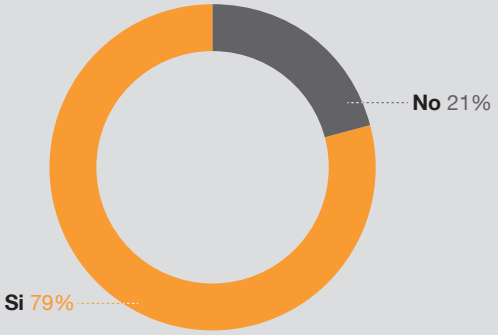
- gestione delle terze parti;
- *Policy Data Retention;*
- gestione degli strumenti di lavoro.

Tutte le aziende rispondenti alla survey hanno dichiarato di aver definito una o più procedure in ambito Data Protection. In particolare, dichiarano di aver regolamentato:

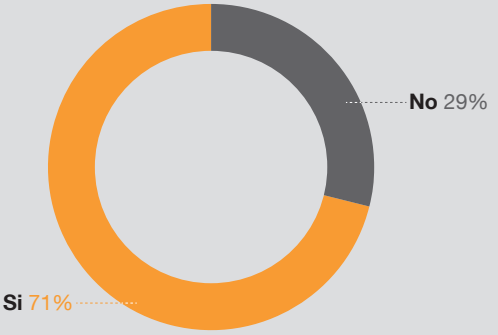
Data breach



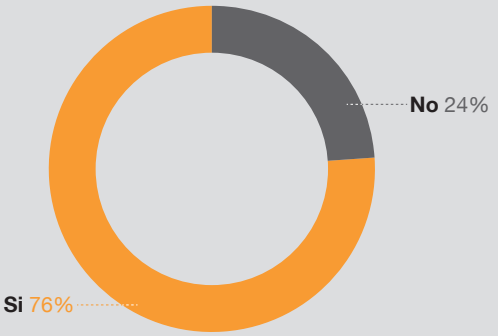
Diritti di accesso



Privacy by design/by default

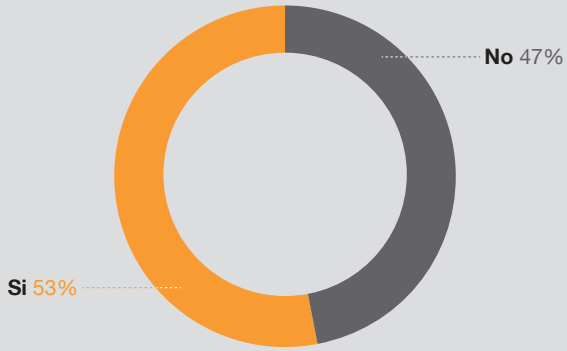


DPIA

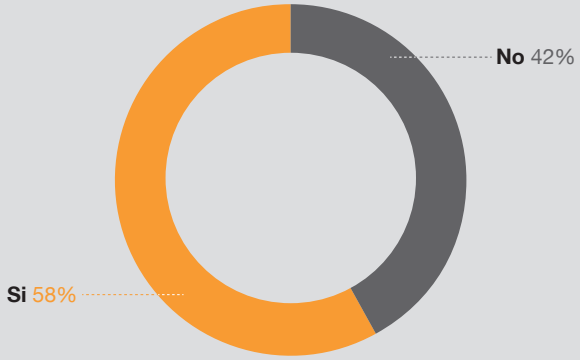


È stata definita una policy di Data classification?

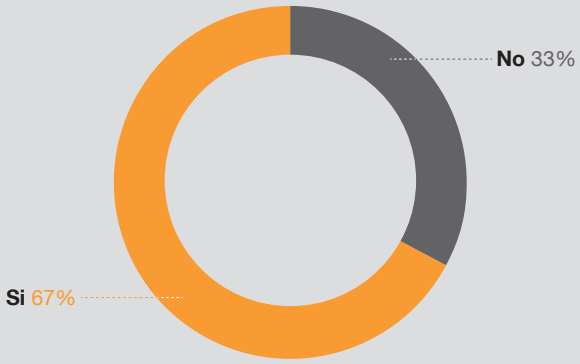
Alto



Medio



Basso



Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

La *policy di* ***Data Classification*** è finalizzata a garantire la **riservatezza**, l'**integrità** e la **disponibilità dei dati e documenti**, «etichettandoli» in base alla criticità e all'impatto che essi hanno sul business. Ogni livello di classificazione dei dati e dei documenti deve essere associato a una serie di **misure di sicurezza** di base che forniscono una protezione adeguata contro vulnerabilità, minacce e rischi.

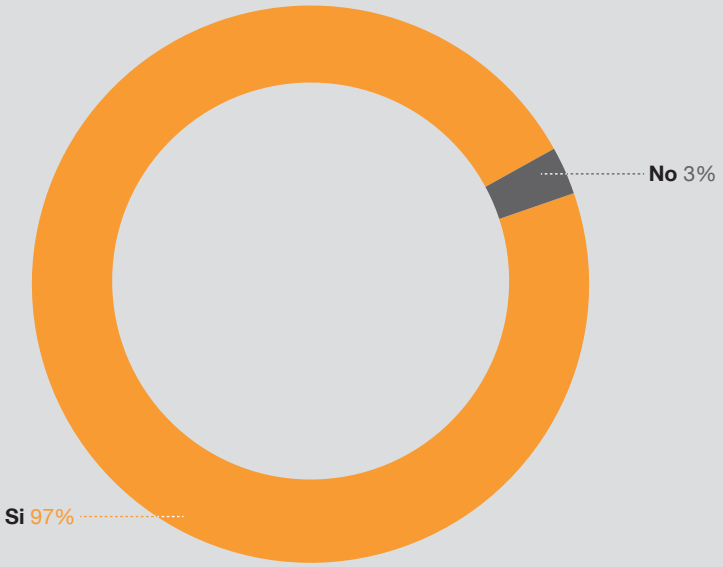
Il **42%** dei rispondenti alla survey dichiara di non essersi dotato di una *policy* di *Data Classification*.

05 Diritti dell’interessato

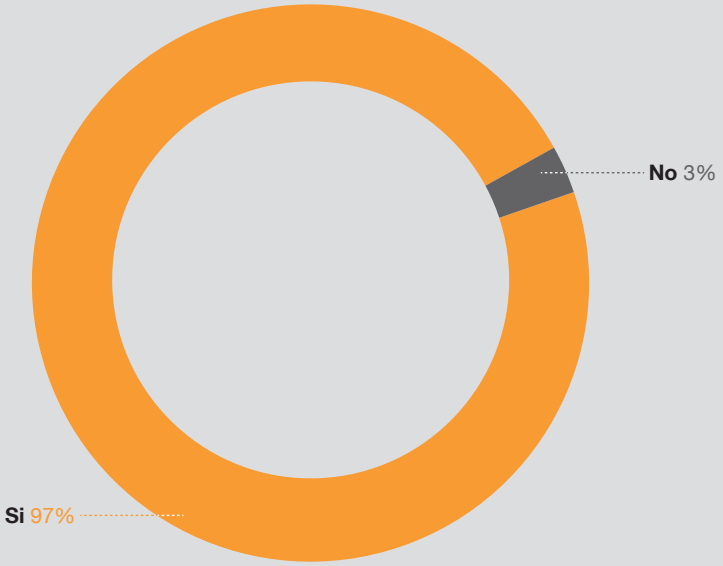
Al fine di garantire la protezione e la riservatezza dei dati personali degli interessati, il GDPR, secondo quanto statuito negli artt. 13 e 14, conferisce ai soggetti interessati diritti, mediante i quali gli stessi possono assicurarsi che i propri dati personali non vengano utilizzati in modo improprio e per finalità diverse dallo scopo legittimo per il quale sono stati originariamente forniti.

Il **97%** delle aziende rispondenti alla survey dichiara di aver redatto e divulgato agli interessati delle apposite informative, e che tali documenti sono adeguatamente archiviati al fine di dimostrare a potenziali stakeholders l'esistenza degli stessi.

Sono state redatte e rese note agli interessati apposite informative ex artt. 13 e 14 GDPR? L'interessato riceve sempre le suddette informative?



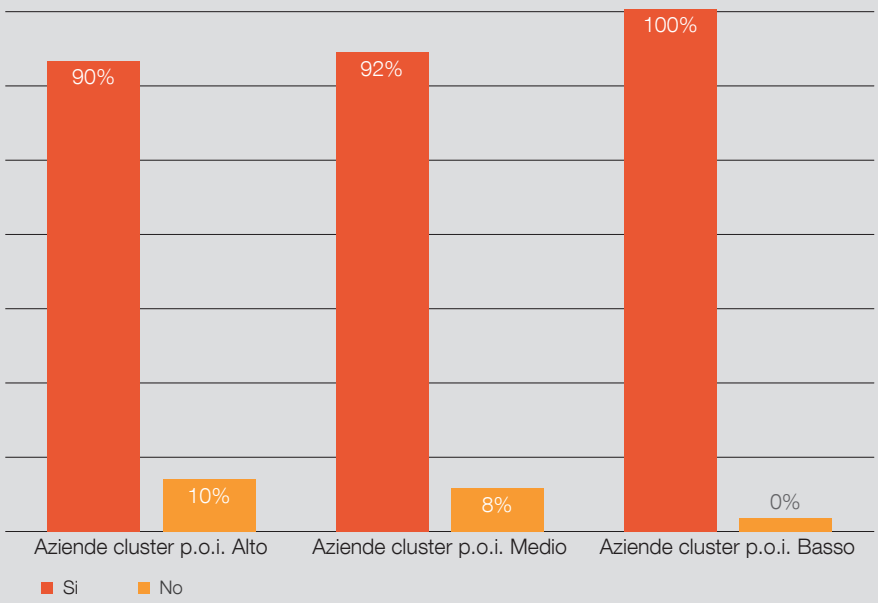
Qualora un trattamento di dati personali si fondi sul consenso dell'interessato, è possibile dimostrare l'esistenza del consenso?



06 Ruoli e responsabilità

In media, circa il **92%** delle aziende rispondenti alla survey ha dichiarato di aver definito all'interno della propria organizzazione una specifica struttura dedicata alla gestione delle tematiche di Data Protection.

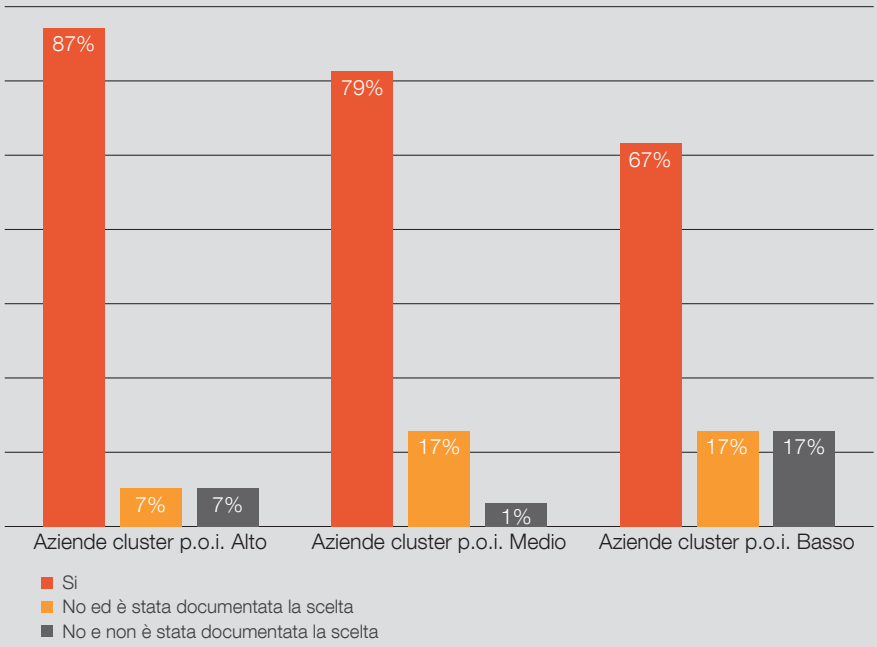
È stata definita e formalizzata una struttura privacy atta a supportare i dipendenti nello svolgimento dell'attività lavorativa sulle tematiche di data protection?



Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

A seguito dell'adeguamento ai requisiti introdotti dal GDPR, sono state svolte specifiche sessioni di formazione sui temi specifici del GDPR e di Data Protection?



Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

Con l'entrata in vigore del GDPR è stata introdotta la figura professionale del *Data Protection Officier* (DPO), il cui compito principale è quello di osservare, valutare e organizzare la gestione del trattamento di dati personali e la loro protezione all'interno di un'azienda (sia essa pubblica che privata).

A tale proposito:

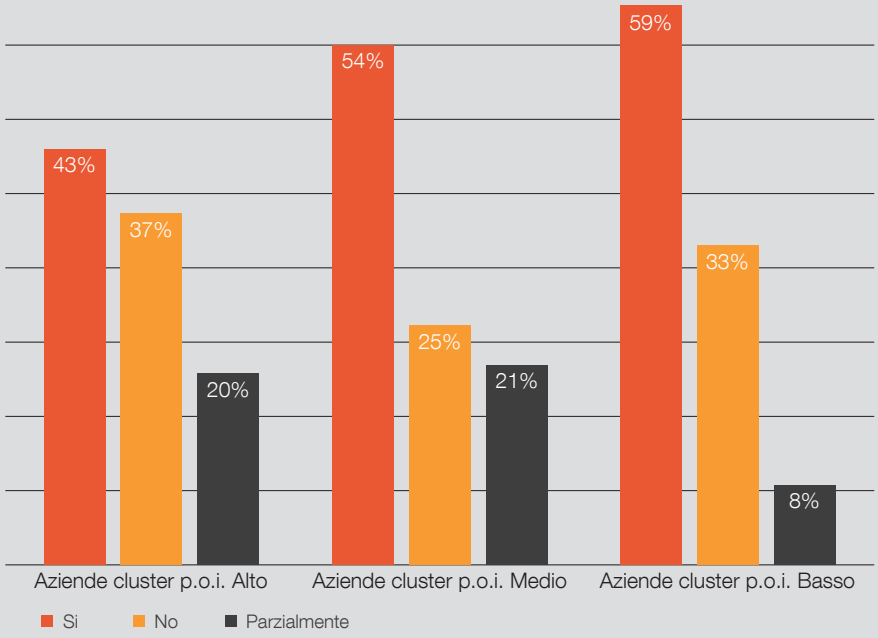
- il **20%** delle aziende rispondenti alla survey dichiara di non aver nominato un DPO;
- il **7%** delle aziende classificate con *privacy overall impact* "alto" dichiara di non aver documentato tale scelta.

Circa il **32%** delle aziende rispondenti alla survey dichiara di non aver previsto specifiche e periodiche attività di monitoraggio sui soggetti terzi identificati come «Responsabili» del trattamento.

Circa il **18%** delle aziende (opzione di risposta «Parzialmente») dichiara che:

- non ha nominato i Responsabili al trattamento;
- è in fase di identificazione delle attività di monitoraggio più appropriate;
- ha identificato le attività di monitoraggio, ma non le ha ancora poste in essere.

Sono previste specifiche e periodiche attività di monitoraggio dei soggetti terzi identificati come “Responsabili” del trattamento?



Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

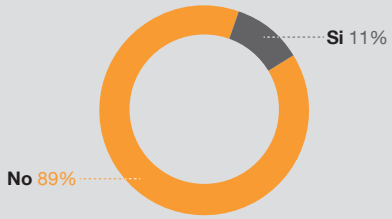
Il GDPR attribuisce in capo al Titolare la responsabilità in caso di mancato rispetto della norma da parte dei soggetti nominati «Responsabili» del Trattamento; pertanto, il Titolare deve monitorare l'operato del Responsabile.

L'**11%** delle aziende rispondenti alla survey dichiara di non aver effettuato nessun tipo di valutazione sui responsabili esterni.

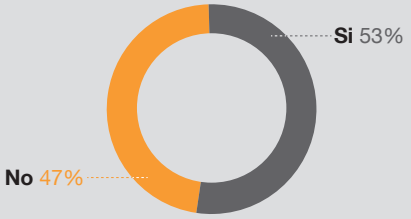
Il **3%** dichiara di aver effettuato un monitoraggio mediante l'ottenimento di un report di attestazione (es. Service Organization Controls, SOC).

Quali strumenti sono stati utilizzati per la valutazione dell'affidabilità, dal punto di vista data protection, per i soggetti identificati come "responsabili" (esterni) del trattamento?

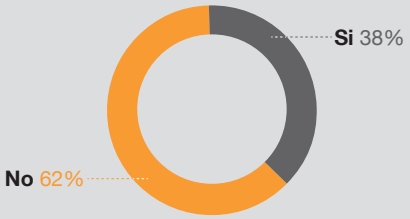
Nessuna valutazione



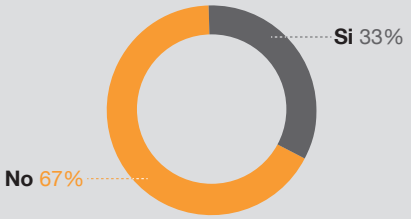
Checklist



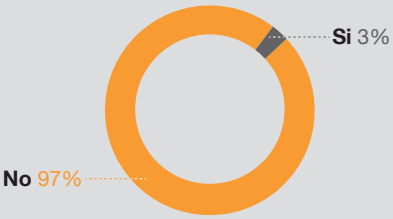
Valutazione qualitativa



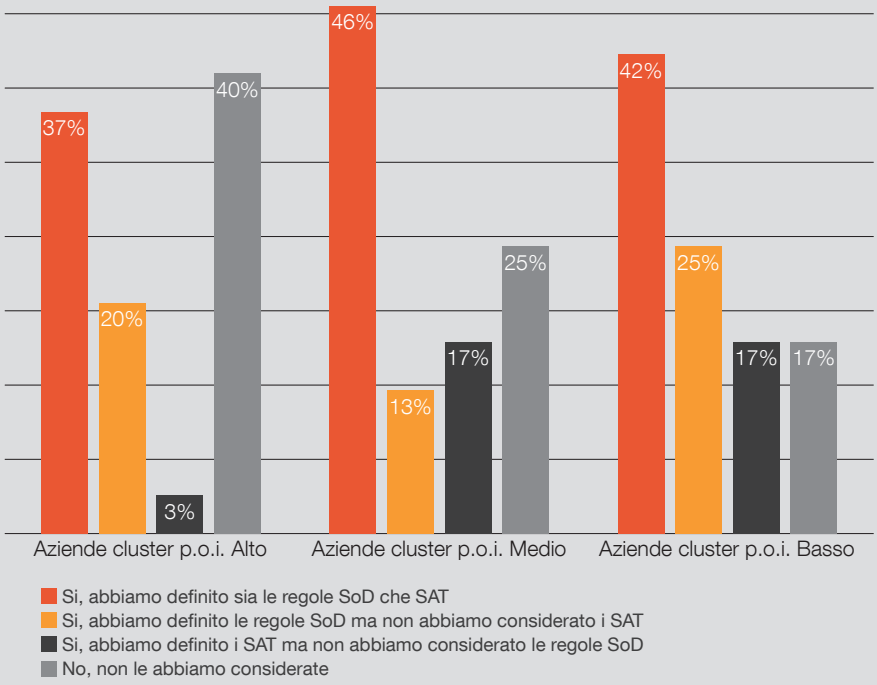
Set di misure di sicurezza



Ottenimento di un report di attestazione (es. SOC2)



Su quale ambito in materia di Data Protection si è posta maggiore attenzione per la valutazione degli impatti e sono state messe in atto adeguate misure di salvaguardia?



Il **70%** delle aziende rispondenti alla survey dichiara di aver posto attenzione per la valutazione degli impatti su almeno un ambito in materia di Data Protection e di aver messo in atto adeguate misure di sicurezza.

In particolare:

- il **40%** dichiara di aver definito sia regole di Segregation of Duties (SoD) che in ambito Sensitive Access Transactions (SAT);
- il **30%** dichiara di aver definito o le sole regole SoD o le sole regole SAT.

Legenda clusterizzazione rispondenti

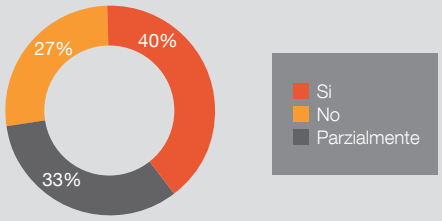
- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

Il **52%** delle aziende rispondenti alla *survey* (appartenenti a cluster diversi) dichiara di non aver attribuito ruoli, compiti e responsabilità per l'eventuale gestione di un'eventuale visita ispettiva dell'Autorità Garante.

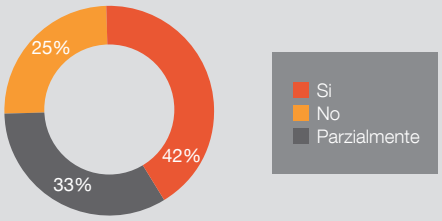
Il **92%** delle aziende classificate nel cluster con *privacy overall impact* "basso", tuttavia, dichiara di aver attribuito - in tutto o in parte - ruoli, compiti e responsabilità per la gestione di eventuali visite ispettive dell'Autorità.

Sono stati definiti formalmente (ad es. tramite una procedura interna) ruoli, compiti e responsabilità da attribuire in ipotesi di visita ispettiva dell'Autorità Garante?

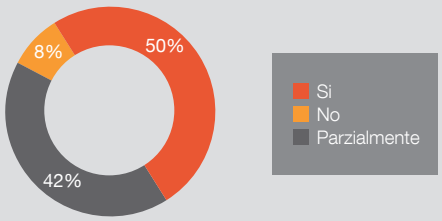
Alto



Medio



Basso



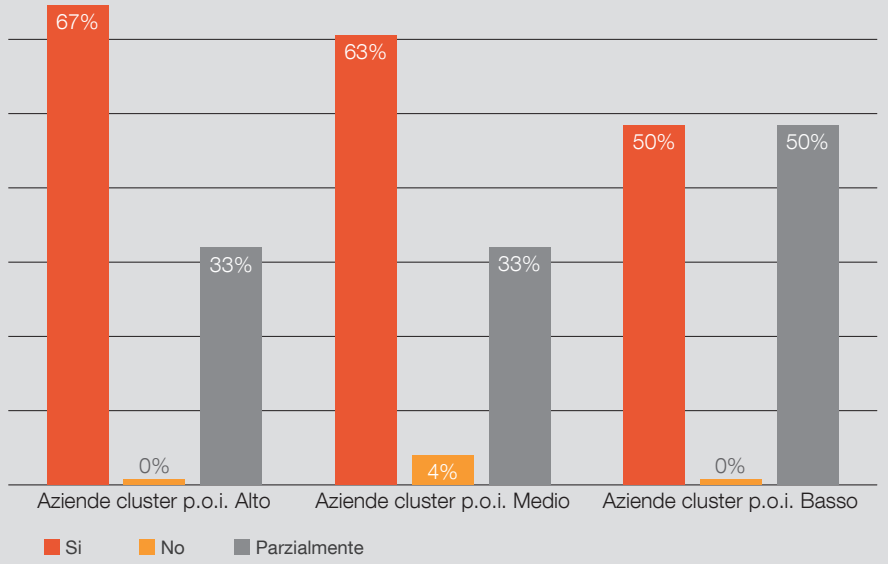
Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

07 Misure di sicurezza

In media il **35%** delle aziende rispondenti alla *survey* appartenenti ai tre cluster dichiara di non aver implementato misure di sicurezza idonee coerentemente a quanto stabilito nell'art.32* del Regolamento.

Sono state implementate le misure di sicurezza idonee (art. 32) come richiamato dal Regolamento (tra cui anonimizzazione, crittografia, ecc.)?

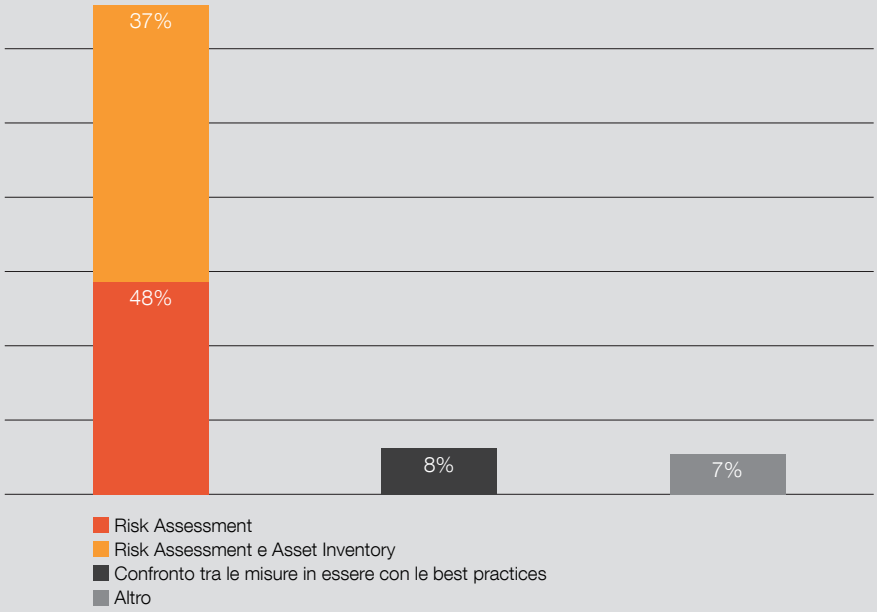


Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

*L'Art. 32 par. 1 del GDPR, afferma che: «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.».

Quali sono state le “metriche” adoperate al fine di valutare l’adeguatezza delle misure di sicurezza applicate ai sistemi sottostanti i trattamenti di dati personali in essere?



L’**85%** circa delle aziende rispondenti alla *survey* dichiara di aver svolto un *Risk assessment* (di queste il **48%** delle aziende dichiara di aver svolto anche l’*asset inventory*).

Il **15%** delle aziende rispondenti dichiara di aver valutato le misure di sicurezza per mezzo di altri strumenti.

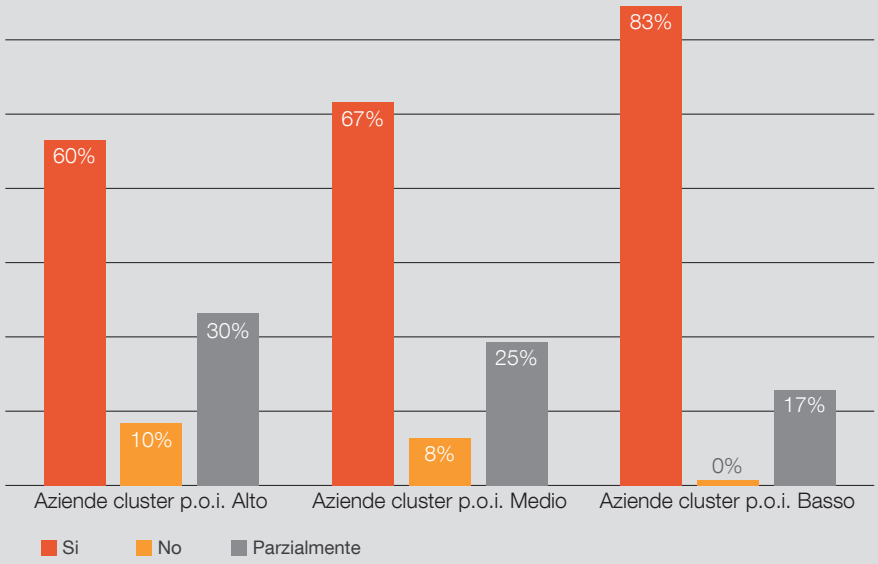
Best practice

L’identificazione ed il censimento dei dati aziendali intesi come asset a sostegno del business (cd.asset inventory) è uno strumento di IT Risk management e ha lo scopo di censire le tipologie di dati (es. finanziari, personali, strategici, ecc.) in uso in Azienda, la relativa natura (digitale, cartacea o entrambe), definirne la «criticità» e le misure di sicurezza adeguate a proteggerli e definite in via «proporzionale» al livello di criticità degli stessi.

Il **67%** delle aziende rispondenti alla *survey* dichiara di aver attuato una procedura finalizzata alla valutazione del rischio *privacy* derivante dalle nuove attività di trattamento o dalle modifiche intervenute ai trattamenti già in essere.

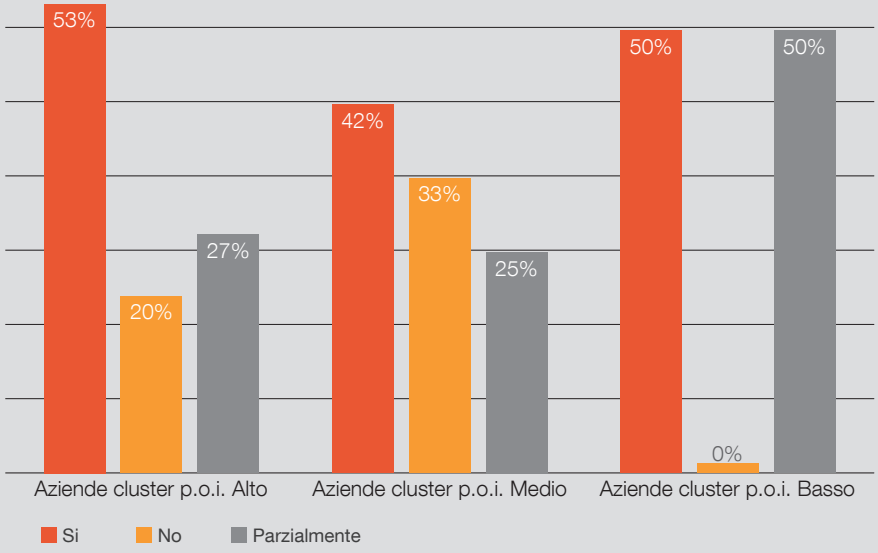
Il **26%** delle aziende dichiara di aver parzialmente posto in essere tale procedura.

È prevista ed attuata una procedura finalizzata a valutare il rischio privacy derivante dalle nuove attività di trattamento o dalle modifiche intervenute ai trattamenti già in essere?



il **48%** delle aziende dichiara di aver valutato le misure di sicurezza applicate in ambito “mobile device” aziendali.

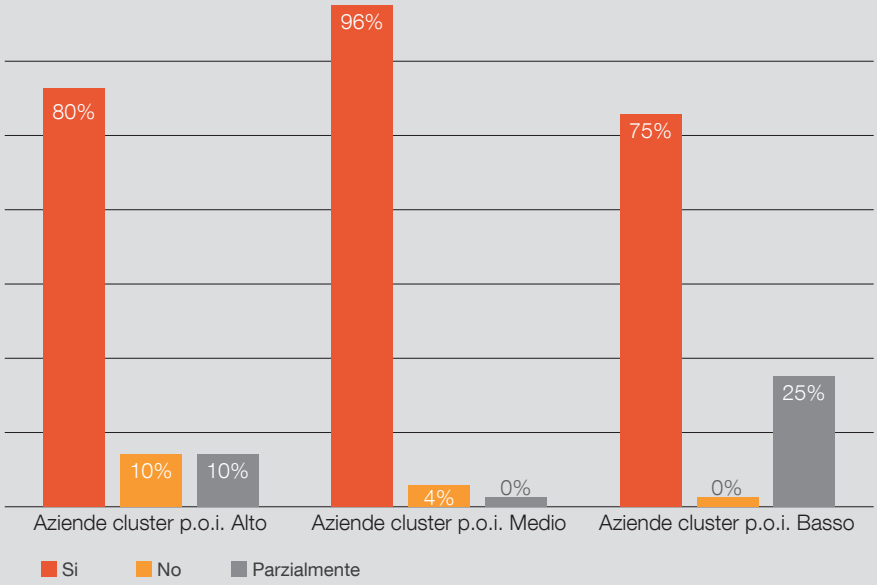
È stato svolto un assessment volto a verificare l’adeguatezza delle misure di sicurezza applicate ai mobile device aziendali (smartphone, tablet, ecc.)?



Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

E’ previsto un registro finalizzato a censire e documentare le violazioni (data breach)?



L’**85%** delle aziende rispondenti alla *survey* dichiara di aver predisposto un registro finalizzato a censire e documentare le violazioni (*data breach*).

In particolare, l’**80%** delle aziende classificate con *privacy overall impact “alto”* dichiara di aver ritenuto opportuno documentare e storicizzare tutti i *data breach* definendo così una *knowledge base* consultabile in caso di necessità.

Best practice

Per svolgere un assessment volto a verificare l’adeguatezza delle misure di sicurezza applicate ai mobile device aziendali è opportuno indagare le seguenti aree:

- ***Governance***
- ***Remote Access***
- ***Data Loss***
- ***Malware***
- ***Incident Response***

Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

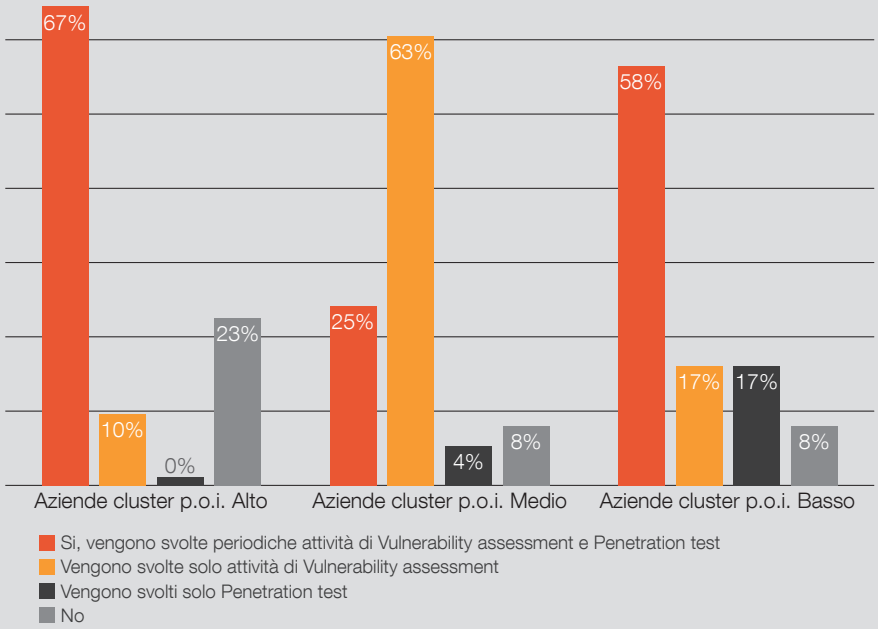
Il **64%** delle aziende rispondenti alla *survey* dichiara di svolgere con cadenza periodica sia *Vulnerability Assessment* (VA) che *Penetration Test* (PT).

Il **15%** delle aziende rispondenti alla *survey* dichiara di svolgere periodicamente solo *VA* o *PT*.

Il **21%** delle aziende rispondenti alla *survey* dichiara non aver effettuato alcun tipo di attività in tale ambito.

Si sottolinea che il **23%** circa delle aziende classificate nel cluster con *privacy overall impact "alto"* dichiara di non avere ancora posto in essere e/o non ha ancora previsto di porre in essere delle azioni relativamente a tale ambito.

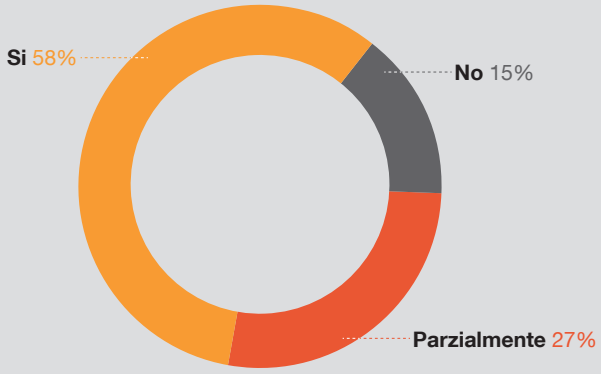
Vengono svolte periodiche attività di vulnerability assessment (VA) e penetration test (PT) sui sistemi che trattano dati personali?



Legenda clusterizzazione rispondenti

- Privacy overall impact Alto: Healthcare, Consumer services, Consumer goods
- Privacy overall impact Medio: Financial, Technology e Energy & Utilities
- Privacy overall impact Basso: Industrials

Sono monitorate periodicamente le attività poste in essere dagli utenti con profilo di Amministratore di Sistema (AdS)/Amministratore di database (DBA)?



Il **58%** delle aziende rispondenti alla *survey* dichiara di monitorare periodicamente le attività poste in essere dagli Amministratori di Sistema (AdS) e Amministratori di Database (DBA).

Best practice

Verifica delle attività: L´operato degli amministratori di sistema dovrebbe essere oggetto, con cadenza almeno annuale, di un´attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Registrazione degli accessi: Dovrebbero essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

08 Sintesi

Sulla base di quanto dichiarato dalle aziende rispondenti alla survey, per gli ambiti inerenti a:

- ***contesto generale Privacy;***
- ***principi;***
- ***diritti dell'interessato.***

è stata riscontrata una sostanziale omogeneità delle azioni intraprese dalle aziende nel processo di adeguamento al GDPR, mentre per gli ambiti inerenti a:

- ***ruoli e responsabilità;***
- ***misure di sicurezza.***

è stata riscontrata una sostanziale eterogeneità delle azioni intraprese.

Prevediamo di monitorare il processo di adeguamento al GDPR anche nel prossimo anno.

Contatti

Nicola Monti

Partner
Risk Assurance Leader

+39 348 2504036
nicola.monti@pwc.com

Andrea Lensi

Partner
PwC TLS

+39 347 9162891
andrea.lensi@pwc.com

Dino Ponghetti

Associate Partner
Risk Assurance
Coordinatore Digital Risk Solutions

+39 348 1505207
dino.ponghetti@pwc.com

Luigi Lodigiani

Associate Partner
Risk Assurance

+39 348 8519825
luigi.lodigiani@pwc.com