



## **CYBERSECURITY & PRIVACY**

**gap e margini di convergenza tra gli addetti ai lavori**

*(Novembre 2023)*

**a cura dell'Osservatorio di Federprivacy**

Gli addetti ai lavori che si occupano di protezione dei dati nelle organizzazioni pubbliche e private hanno a che fare con una materia trasversale e multidisciplinare che abbraccia vari ambiti, e questo comporta che degli esperti di tematiche diverse debbano interagire tra di loro, con il rischio però di incontrare delle difficoltà dovute ai differenti background. Infatti, quando sono chiamati a confrontarsi a un tavolo di lavoro, di solito gli esperti di protezione dei dati tendono a focalizzarsi sulle proprie specifiche competenze.

Ad esempio, avvocati e Data Protection Officer che hanno un profilo giuridico possono concentrarsi principalmente sugli adempimenti richiesti dal GDPR e sugli aspetti riguardanti la compliance normativa, usando un sofisticato linguaggio *legalese* che risulta di difficile comprensione a chi non è un giurista.

Dall'altra parte, spesso CISO e Security Manager considerano invece prioritaria la sicurezza dei dati, e quando devono rapportarsi con i loro interlocutori possono ricorrere a un gergo tecnico che solo gli informatici possono capire pienamente.

Accade quindi spesso che i professionisti della privacy e quelli della cybersecurity viaggiano su due binari paralleli che raramente si incontrano, ma è evidente che nella nostra era digitale c'è la necessità che gli addetti ai lavori con competenze diverse sappiano comunicare bene e comprendersi tra di loro quando devono affrontare questioni che richiedono soluzioni che al contempo garantiscano un adeguato livello di sicurezza dei dati e soddisfino le prescrizioni delle leggi applicabili.

Consapevole della necessità di comprendere quali sono le maggiori difficoltà che incontrano gli addetti ai lavori, e di individuare le possibili soluzioni per colmare i gap e aiutarli a cooperare meglio tra di loro mentre perseguono il comune obiettivo di proteggere i dati in modo conforme alla normativa vigente, l'Osservatorio di Federprivacy, associazione professionale iscritta presso il Ministero dello Sviluppo Economico (ora Ministero delle Imprese e del Made in Italy) ai sensi della Legge 4/2013, nel mese di novembre 2023 ha condotto un sondaggio composto da 10 domande mirate a cui hanno partecipato complessivamente 1.507 professionisti con competenze diverse.

### ***Le domande poste nel sondaggio***

Ai professionisti intervistati nel sondaggio tramite un questionario sul sito [www.federprivacy.org](http://www.federprivacy.org) con la possibilità di essere identificati tramite autenticazione oppure di rispondere in forma anonima, sono state poste una serie di 10 domande a risposta chiusa, di cui alcune con una sola risposta selezionabile, ed alcune con possibilità di fornire risposta multipla. Ogni partecipante ha avuto inoltre a disposizione anche un campo "note" dove inserire liberamente tutti i propri commenti. Le domande a risposta chiusa riguardavano i seguenti argomenti:

- 1. Background professionale dei partecipanti**
- 2. Aspetti più importanti per un tavolo di lavoro che valuta questioni sulla protezione dei dati**
- 3. Aspetti più sottovalutati da un team di esperti che affronta casi sulla protezione dei dati**
- 4. Difficoltà di interazione con esperti che hanno un background diverso dal proprio**
- 5. Incidenza delle valutazioni di un team multidisciplinare sulle decisioni del management**
- 6. Casi in cui un team che si occupa di protezione dei dati espone l'azienda a rischi**
- 7. Come trovare convergenze con professionisti che hanno competenze diverse dalle proprie**
- 8. Cosa dovrebbe fare il management per facilitare le convergenze**
- 9. Cosa sarebbe utile trovare sul mercato per facilitare le convergenze**
- 10. Margini di convergenza tra addetti ai lavori**

### **Considerazioni finali**

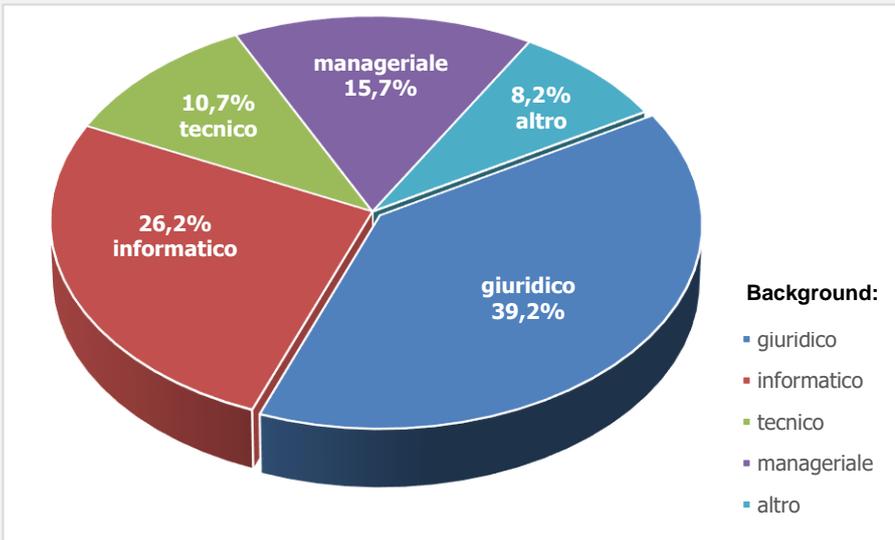
Di seguito i risultati emersi da ciascuna delle 10 domande poste nel sondaggio riguardanti i suddetti aspetti:



## 1. Quale è il tuo background professionale?

Con le risposte ricevute alla suddetta domanda, il seguente grafico (*fig.1*) individua la segmentazione dei diversi profili dei 1.507 professionisti che hanno partecipato al sondaggio, con le relative percentuali ed alcuni commenti obiettivi di interesse per una migliore comprensione del contesto:

**fig.1 – Il background professionale dei partecipanti al sondaggio**



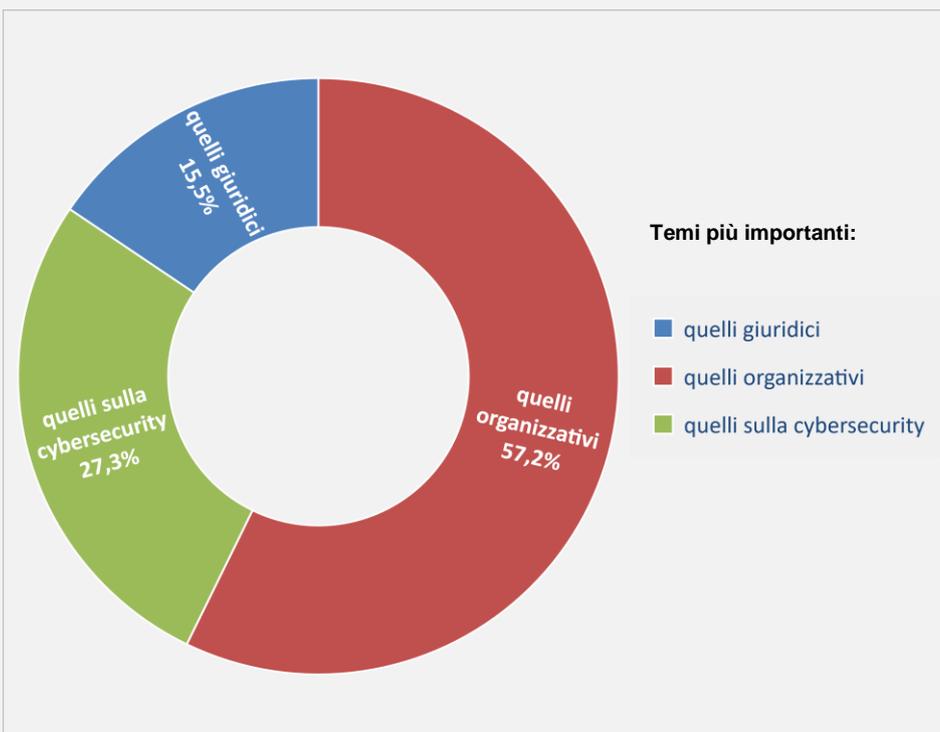
La fig.1 evidenzia che il 39,2% dei partecipanti al sondaggio ha un background giuridico, mentre il 36,9% ha un profilo tecnico, di cui il 26,2% ha specificamente competenze informatiche. Inoltre, il 15,7% di coloro che hanno risposto alle domande sono manager d'impresa, e l'8,2% ha invece altre competenze.

Sia la rilevanza del numero degli addetti ai lavori intervistati (1.507) che l'eterogeneità dei loro profili consente quindi di poter contare su un ampio ventaglio di feedback bilanciati e provenienti da prospettive diverse.

## 2. Quali pensi siano gli aspetti più importanti da affrontare a un tavolo di lavoro che deve valutare una questione riguardante la protezione dei dati?

Come emerge dalla *fig.2*, oltre la metà dei professionisti che hanno partecipato al sondaggio (57,2%) ritiene che quando un tavolo di lavoro deve valutare una questione riguardante la protezione dei dati, gli aspetti più importanti da affrontare sono quelli di carattere organizzativo. Il 27,3% considera invece più importanti i temi della cybersecurity, e il 15,5% quelli giuridici.

**fig.2 – Gli aspetti più importanti da affrontare a un tavolo di lavoro che deve valutare una questione inerente la protezione dei dati**



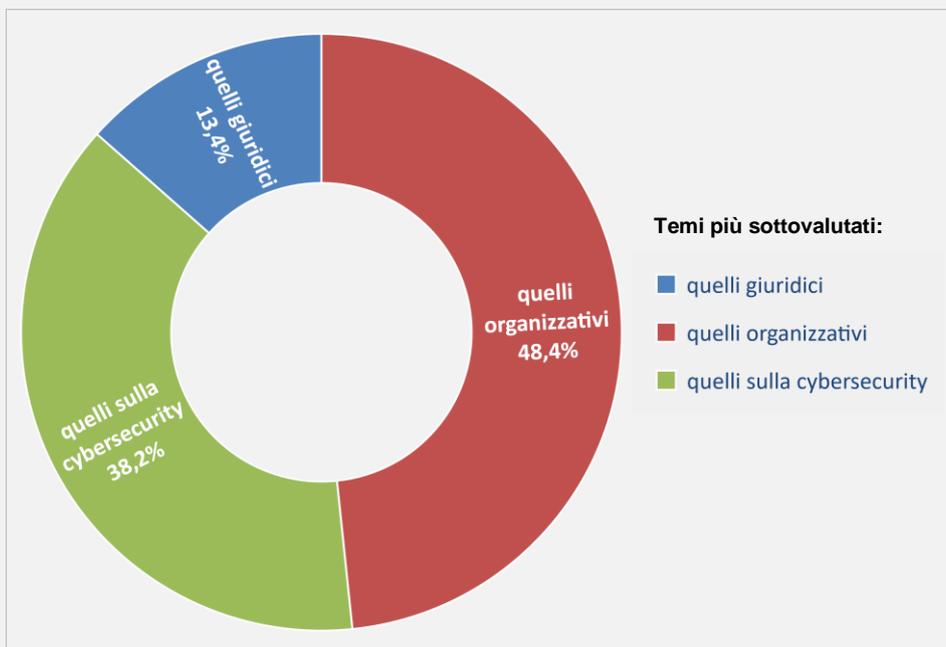
Benché le principali competenze richieste ai professionisti che si occupano di protezione dei dati sono solitamente giuridiche ed informatiche, il fatto che la maggioranza degli intervistati (57,2%) abbia indicato gli aspetti organizzativi come quelli più importanti evidenzia la necessità di avvalersi anche di professionisti esperti di governance aziendale, in particolare di data management e sistemi di gestione della protezione dei dati. Rileva inoltre la prevalenza dell'importanza riconosciuta agli aspetti sulla cybersecurity (27,3%) rispetto a quelli giuridici (15,5%), probabilmente dovuta al crescente numero di attacchi informatici e alla maggiore consapevolezza della necessità di proteggere i dati. In ogni caso, i temi riguardanti il rispetto della normativa sono ritenuti secondari rispetto agli altri.



### 3. Quali pensi siano gli aspetti maggiormente sottovalutati quando un team di esperti si riunisce per una questione riguardante la protezione dei dati?

Come emerge dalla *fig.3*, gli aspetti maggiormente sottovalutati sono quelli organizzativi (48,4%) e quelli sulla cybersecurity (38,2%). Solo il 13,4% dei partecipanti al sondaggio ritiene che i temi giuridici siano sottovalutati.

**fig.3 – Gli aspetti maggiormente sottovalutati quando un team di esperti si riunisce per una questione inerente la protezione dei dati**

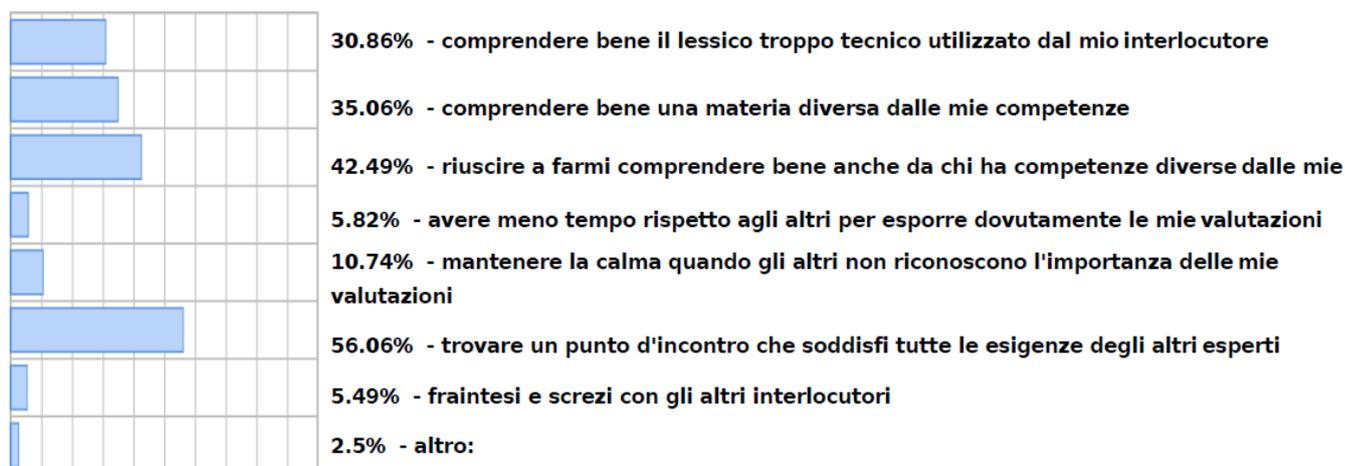


Il fatto che quasi la metà degli addetti ai lavori (48,4%) riconosca che gli aspetti organizzativi vengano sottovalutati dai team che si occupano di protezione dei dati segue evidentemente la tendenza riscontrata al quesito precedente sull'importanza di affrontare tali temi, confermando la necessità di rafforzare la governance dei dati nelle organizzazioni pubbliche e private.

Il basso numero di risposte sugli aspetti giuridici (13,4%) può significare che i team di protezione dei dati li ritengano dovutamente presidiati, mentre d'altra parte è più elevata la percentuale di coloro che reputano più sottovalutati quelli sulla cybersecurity. (38,2%)

### 4. Quando devi interagire con altri esperti di protezione dei dati che hanno un background diverso dal tuo, quali difficoltà ti capita di incontrare?

**fig.4 – Difficoltà incontrate dagli addetti ai lavori quando interagiscono con altri esperti di protezione dei dati con un diverso background**

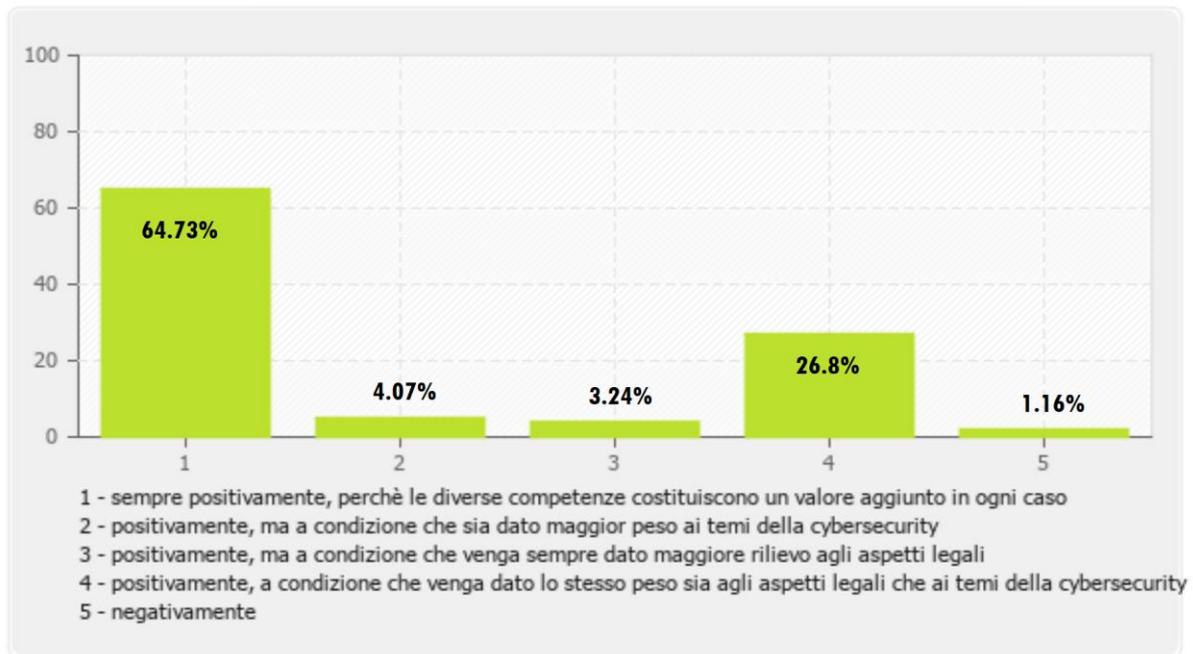


Tenendo conto della complessità dei temi della protezione dei dati, che richiedono di conciliare gli aspetti di compliance normativa con l'effettiva sicurezza dei dati, la *fig.4* rivela che più della metà degli addetti ai lavori (56,06%) incontra difficoltà a trovare un punto d'incontro che soddisfi tutte le esigenze degli altri esperti con un background diverso. Anche la comprensione tra gli esperti rappresenta un problema rilevante, infatti il 42,49% afferma di avere difficoltà a farsi comprendere bene da chi ha competenze diverse dalle proprie, mentre il 35,06% riscontra difficoltà a capire una materia che non è di sua specifica competenza, e il 30,86% fatica anche a comprendere il lessico troppo tecnico usato dal suo interlocutore.



## 5. Come reputi che incidano le valutazioni di un team multidisciplinare sulle decisioni del management aziendale?

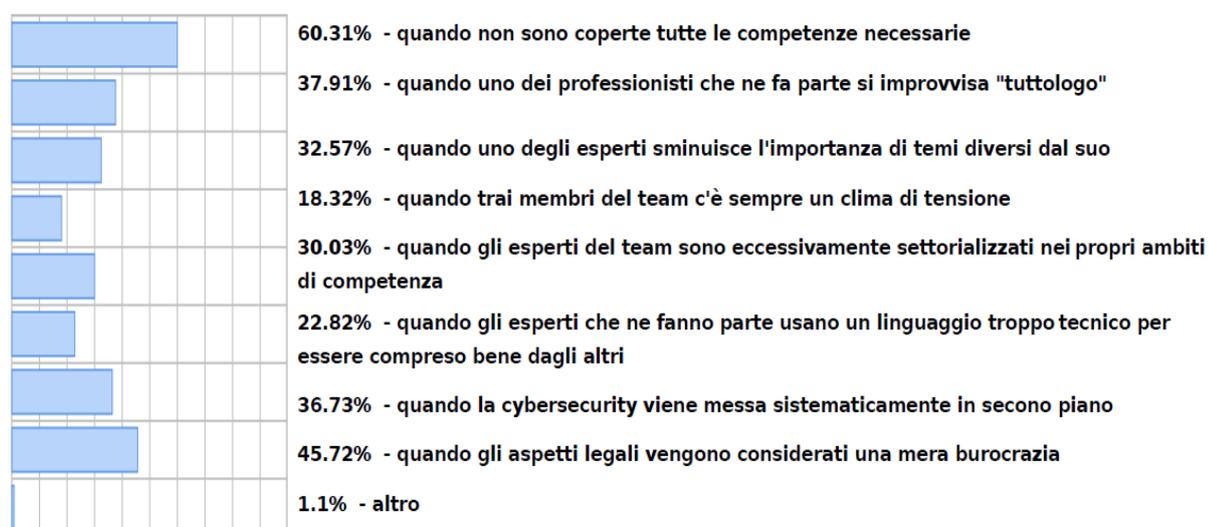
fig.5 – Incidenza delle valutazioni di un team multidisciplinare sulle decisioni del management aziendale



La fig.5 mette in evidenza che, nel complesso, ben il 91,53% degli addetti ai lavori riconosce l'importanza di lavorare in un team multidisciplinare, affermando che le valutazioni da questo effettuate influiscono positivamente sulle decisioni del management. Di questi, il 64% pensa che gli effetti siano sempre positivi, in quanto le diverse competenze costituiscono un valore aggiunto in ogni caso, mentre il 26,8% ritiene che un team multidisciplinare giovi alle decisioni del management solo a condizione che venga dato lo stesso peso tanto alla cybersecurity quanto agli aspetti legali.

## 6. In quali casi pensi che un team che si occupa di protezione dati possa esporre l'azienda a rischi?

fig.6 – Incidenza delle valutazioni di un team multidisciplinare sulle decisioni del management aziendale



Come si evince dalla fig.6, il 60,31% degli addetti ai lavori ritiene che un team che si occupa della protezione dei dati possa esporre l'azienda a rischi quando non sono coperte tutte le competenze necessarie. La carenza di esperti in materia di GDPR e compliance normativa espone infatti un'organizzazione a rischi di sanzioni, mentre la mancanza di professionalità in materia di cybersecurity la espone ad attacchi informatici e conseguenti perdite di dati.





*Sempre dalla fig.6 riportata nella pagina precedente, si rileva che quasi la metà degli addetti ai lavori (45,72%) crede che a esporre l'azienda a rischi possa essere anche un team che considera gli aspetti legali del GDPR e della normativa applicabile come una mera burocrazia, e a 5 anni dall'introduzione del Regolamento europeo risulta che il 78% delle aziende italiane considerano come tale il rispetto del GDPR. (Rif. sondaggio Federprivacy, maggio 2023). Tale concezione, sembra trovare riscontro anche nelle risposte fornite al quesito 2), in cui solo il 15,5% degli addetti ai lavori indica i temi giuridici come quelli più importanti da affrontare.*

*In base al 36,73% delle risposte, possono invece emergere rischi quando è la cybersecurity ad essere messa sistematicamente in secondo piano.*

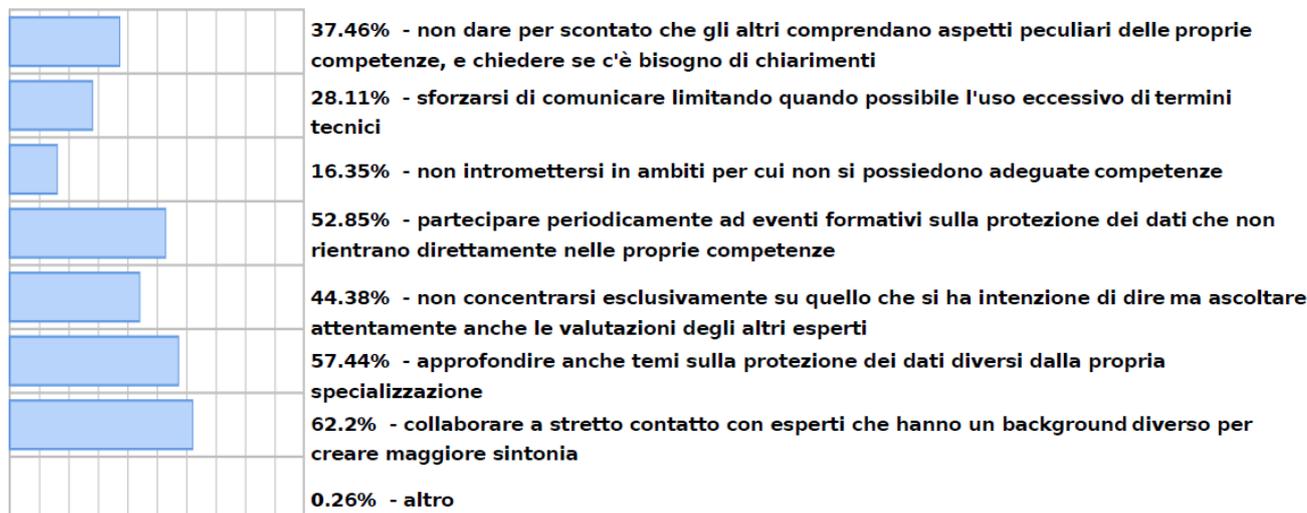
*Secondo il 37,91% di coloro che hanno partecipato al sondaggio, espone a rischi l'azienda anche un professionista del team che si improvvisa "tuttologo". Tale rischio può potenzialmente accentuarsi in modo critico nel caso in cui non siano coperte tutte le competenze necessarie, come rilevato sempre nelle risposte fornite nello stesso quesito.*

*Un professionista su tre (32,57%) afferma che potrebbero verificarsi potenziali ripercussioni negative per l'azienda quando un membro del team sminuisce temi della protezione dei dati diversi dagli ambiti di sua competenza, o (30,03%) quando gli esperti del team sono eccessivamente settorializzati.*

*Quasi uno su quattro (22,82%) considera rischioso il fatto di non comprendersi bene quando gli esperti usano un linguaggio troppo tecnico per essere compreso bene dagli altri professionisti del team, e per il 18,32% possono derivare rischi per l'azienda anche da un clima di continua tensione tra i professionisti.*

## **7. Cosa pensi che potresti fare per trovare maggiori convergenze con altri professionisti con competenze in materia di protezione dei dati diverse dalle tue?**

**fig.7 – Cosa possono fare gli addetti ai lavori per trovare maggiori convergenze con gli altri esperti con competenze diverse dalle proprie**

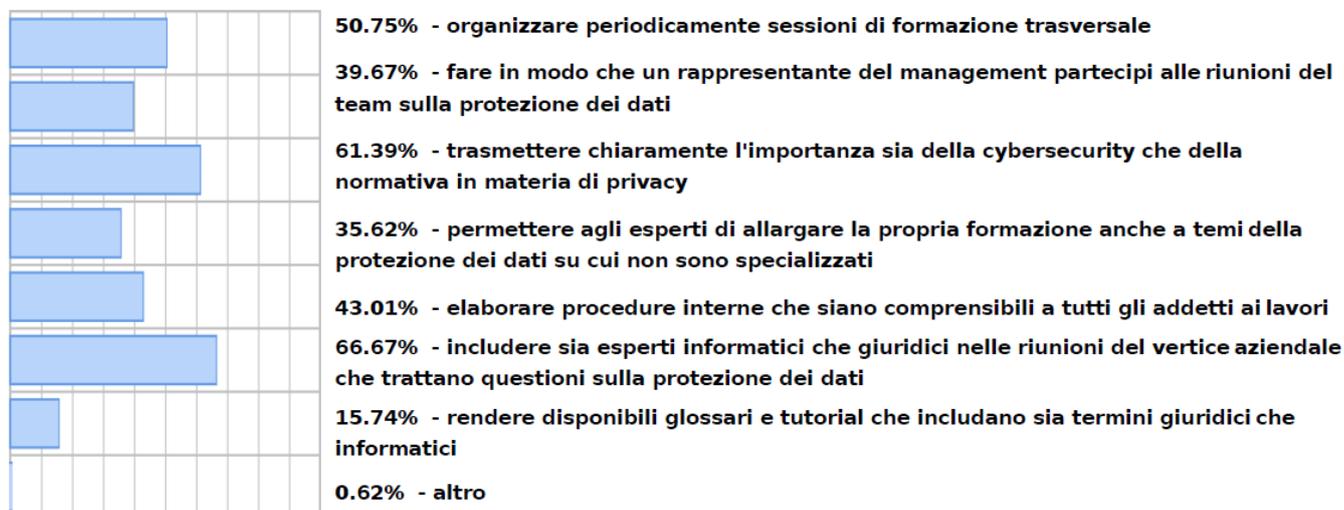


*Analizzando la fig.7 si nota come ben il 62,2% dei professionisti ritiene di poter trovare maggiori convergenze e creare più sintonia tra addetti ai lavori collaborando a stretto contatto con altri esperti che hanno un background diverso dal proprio. Oltre la metà pensa che sia necessario approfondire anche temi diversi dalla propria specializzazione (57,44%) e partecipare periodicamente ad eventi formativi sulla protezione dei dati che non rientrano direttamente nelle proprie competenze (52,85%). A livello relazionale, il 44,38% pensa che si debba evitare di concentrarsi solo sulle proprie valutazioni, ascoltando invece con attenzione quelle degli altri esperti. Inoltre il 37,46% dei partecipanti suggerisce di non dare per scontato che gli altri comprendano aspetti peculiari delle proprie competenze, rendendosi disponibili a fornire gli eventuali chiarimenti necessari. Un terzo (28,11%) di coloro che hanno risposto concorda sul fatto che occorra sforzarsi di comunicare limitando quando possibile l'uso eccessivo di termini tecnici per facilitare la comprensione. Nel 16,35% dei casi viene dato anche il consiglio di non intromettersi in ambiti per cui non si possiedono adeguate competenze.*



## 8. Cosa pensi dovrebbe fare il management di un'azienda per facilitare le convergenze tra professionisti con competenze diverse che si occupano di protezione dei dati?

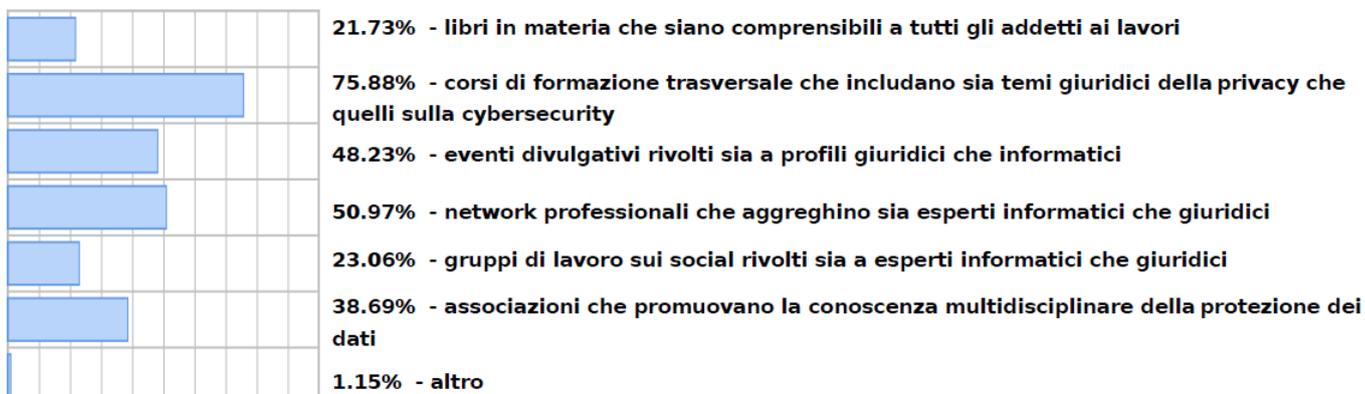
fig.8 - Cosa può fare il management per facilitare le convergenze tra gli addetti ai lavori che si occupano della protezione dei dati



Analizzando la fig.8 si osserva che il 66,67% degli esperti informatici e/o giuridici vorrebbe essere coinvolto nelle riunioni del vertice aziendale che trattano questioni che hanno un impatto sulla protezione dei dati, mentre il 39,67% vorrebbe che un rappresentante del management partecipasse alle riunioni del team che si occupa della protezione dei dati. Il 61,39% si aspetterebbe dal vertice aziendale che trasmettesse chiaramente l'importanza sia dei temi della cybersecurity che di quelli della normativa sulla privacy. La metà (50,75%) degli addetti ai lavori vorrebbe che la direzione organizzasse periodicamente sessioni di formazione trasversale che contempli tutte le tematiche della protezione dei dati, e il 35,62% di essi desidererebbe di poter allargare la propria formazione anche a temi della protezione dei dati diversi da quelli su cui sono già competenti. Il 43,01% riprende anche i temi della governance, suggerendo procedure interne sulla protezione dei dati che siano comprensibili a tutti gli addetti ai lavori, mentre il 15,74% considera utili anche glossari e tutorial che includano sia termini giuridici che informatici.

## 9. Cosa pensi che sarebbe utile trovare sul mercato per essere facilitato a trovare convergenze tra tutti gli addetti ai lavori della protezione dei dati?

fig.9 - Cosa potrebbe essere utile trovare sul mercato per facilitare le convergenze tra gli addetti ai lavori che si occupano della protezione dei dati

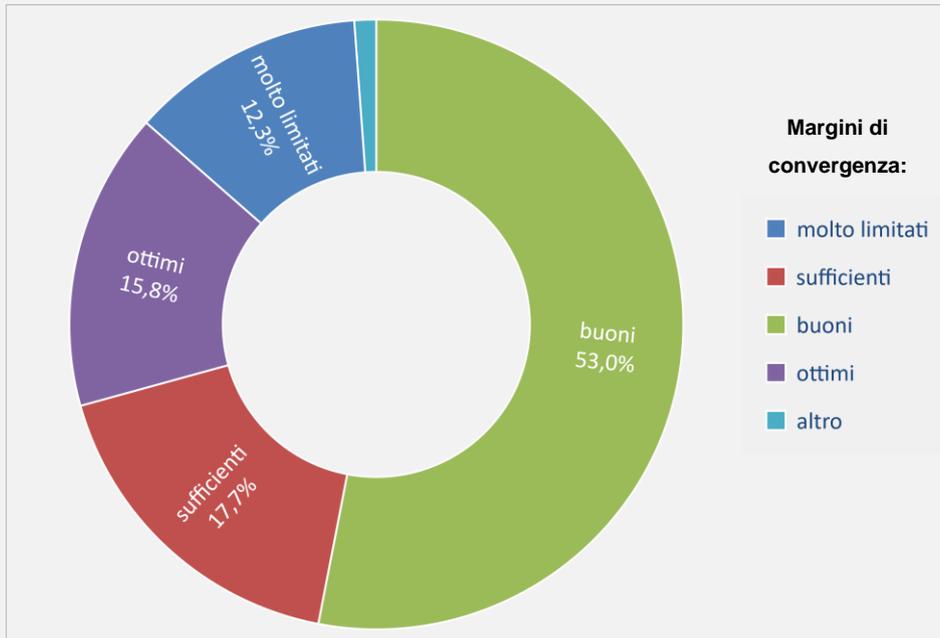


Dalle risposte fornite nella fig.9 si evince che il 75,88% degli addetti ai lavori avverte la necessità di trovare corsi di formazione trasversale che includano sia temi giuridici della privacy che quelli sulla cybersecurity, e la metà (50,97%) vorrebbe far parte di network professionali che aggregino sia esperti informatici che giuridici, mentre il 48,23% è interessato a eventi divulgativi trasversali. Per il 38,69% sono importanti anche le associazioni che promuovono la conoscenza multidisciplinare della protezione dei dati, mentre solo a 1 su 5 (21,73%) interessa leggere libri su tali temi.



## 10. Che margini di convergenza pensi ci siano realisticamente tra gli addetti ai lavori della cybersecurity e quelli della normativa sulla privacy?

fig .10 – I potenziali margini di convergenza tra gli addetti ai lavori della cybersecurity e quelli della normativa sulla privacy



Su 1.507 partecipanti al sondaggio, più della metà (53%) è ottimista e ritiene che ci siano buoni margini di convergenza tra gli addetti ai lavori della protezione dei dati, mentre il 15,8% pensa che si possano raggiungere ottimi risultati. Sono il 17,7% quelli più cauti che credono che i margini siano più contenuti, mentre gli scettici sono il 12,3%.

### Considerazioni finali

Rispetto al passato, gli attuali scenari della protezione dei dati sono sempre più complessi, sia per quanto riguarda la compliance normativa a causa dei numerosi atti normativi emanati dall'Unione Europea dopo il GDPR e delle leggi nazionali che impattano sui trattamenti di dati, sia sul fronte della cybersecurity a causa delle continue evoluzioni di tecnologie come l'intelligenza artificiale che comportano maggiori criticità nella gestione dei dati, e che possono esse stesse essere utilizzate dai cyber criminali nell'ambito di attacchi informatici.

Tale contesto contribuisce peraltro a sfumare i confini tra compliance e cybersecurity, e richiede necessariamente che i temi della protezione dei dati vengano affrontati con un approccio multidisciplinare e trasversale avvalendosi nella maggior parte dei casi di team di esperti giuridici per la compliance e informatici per la cybersecurity, i quali tuttavia incontrano difficoltà ad interagire tra di loro a causa dei loro differenti background, pur riconoscendo nel complesso (91,53%) che le diverse competenze costituiscono un valore aggiunto per il team, e che nel caso in cui non fossero coperte tutte le competenze necessarie l'azienda sarebbe esposta a rischi di sanzioni e violazioni dei dati. (60,31%)

Le suddette difficoltà nella cooperazione e nel coordinamento tra gli addetti ai lavori diventano tangibili anche dalle risposte fornite da oltre la metà degli esperti (57,2%), i quali hanno indicato gli aspetti organizzativi come quelli più importanti per un team che si occupa della protezione dei dati, ma anche quelli più sottovalutati nel 48,4% dei casi, denotando la necessità di implementare le strategie di governance dei dati in modo da superare le difficoltà riscontrate dal 56,06% degli intervistati nel conciliare gli aspetti di compliance normativa con quelli dell'effettiva sicurezza dei dati ed essere in grado di trovare un punto d'incontro che soddisfi tutte le esigenze dei professionisti del team.

Da parte loro, gli addetti ai lavori sono ottimisti sui potenziali margini di convergenza (53%) e ritengono di poter contribuire ad attenuare i gap trovando maggiori convergenze collaborando a stretto contatto con altri esperti che hanno un background diverso dal proprio (62,2%), approfondendo temi diversi dalla propria specializzazione (57,44%) e partecipando ad eventi formativi che non rientrano direttamente nelle proprie competenze (52,85%).

Gli stessi addetti ai lavori informatici e giuridici vorrebbero essere inoltre coinvolti nelle riunioni del vertice aziendale che trattano questioni sulla protezione dei dati (66,67%), e sul mercato ricercano corsi di formazione trasversale che includano sia temi giuridici della privacy che quelli sulla cybersecurity (75,88%).