

LINK: <https://www.lefonti.legal/privacy-gdpr/>

IL NETWORK DI LE FONTI | FINANZA & DIRITTO | WORLD EXCELLENCE | LE FONTI LEGAL | IAIR REVIEW | LE FONTI CEO SUMMIT | LE FONTI AWARDS ITALY | LE FONTI TV | LE FONTI BUSINESS CHANNEL | NEW INSURANCE | NEW PHARMA | Ricerca

NEWASSET MANAGEMENT

LE FONTI LEGAL

LA RIVISTA N°1 DEGLI AVVOCATI

HOME MANDATI ▾ MERCATO LEGALE ▾ RANKING ▾ INTERVISTE ▾ TAVOLE ROTONDE LE FONTI LEGAL TV LE FONTI AWARDS EVENTI **ABBONATI**

SIGN UP LOGIN

Home » Mercato legale » Attualità » La nuova privacy compie un anno, ma l'adeguamento è a ostacoli

La nuova privacy compie un anno, ma l'adeguamento è a ostacoli

ATTUALITÀ



[in](#) LinkedIn [f](#) Share [t](#) Tweet [✉](#) Email

Il nuovo regolamento europeo sulla privacy compie un anno. Attualmente, solo un'azienda su cinque si è adeguata al Gdpr, il 59% ha però progetti in corso e l'88 per cento delle imprese, il 30% in più rispetto a un anno fa, ha un budget dedicato.

Sono numeri in chiaro-scuro quelli resi noti di recente dall'Osservatorio del Politecnico di Milano, che raccontano come da un lato si sia diffusa la consapevolezza, da parte delle imprese italiane, rispetto all'importanza di investire nella privacy. Dall'altra, però, il processo di adeguamento alle nuove norme è ancora lungo, e alla finestra ci sono le verifiche (e soprattutto le sanzioni) annunciate dal Garante privacy. È quanto emerge, tra l'altro, dalla ricognizione effettuata da Le Fonti Legal a un anno dall'entrata in vigore del nuovo regolamento privacy, attraverso le testimonianze raccolte tra i professionisti maggiormente coinvolti dalla normativa: gli avvocati esperti di privacy che stanno

EVENTI

Non ci sono eventi

IN EDICOLA

LE FONTI LEGAL
LA RIVISTA N°1 DEGLI AVVOCATI

IMPRESE IL CODICE DELLA DISCORDIA

Powered by Digi...

LIBRO D'ORO



assistendo le imprese nel processo di adeguamento, i penalisti e i general counsel.

Secondo **Massimiliano Masnada** di Hogan Lovells, «ad un anno dall'entrata in vigore del Gdpr molte imprese stanno adeguando non solo le informative e le nomine a incaricato o responsabile, ma soprattutto i loro sistemi informatici e le loro procedure interne. Tutto ciò ha un costo, necessita di investimenti e di programmazione. Questo è stato un anno di transizione anche perché, almeno in Italia, molte imprese, incluse quelle pubbliche che sono soggette alle stesse regole delle imprese private, non erano preparate considerando la compliance privacy come un costo e non come un'opportunità e una risorsa. Si aggiunga che è stata introdotta in Italia per la prima volta la figura del Dpo che, essendo una figura nuova nei modelli consolidati di corporate governance aziendale, ha suscitato qualche perplessità e incomprensione. La mia previsione è che nel corso del 2019 si consolideranno numerose esperienze ed arriveremo ad un buon livello di cultura aziendale della privacy, almeno per le imprese più grandi e con maggiore visibilità». «Credo che le maggiori difficoltà siano derivate proprio dall'introduzione della figura del Dpo come ulteriore soggetto deputato al controllo di compliance interna in un mondo, come quello finanziario, già caratterizzato da numerose figure di controllori e auditors», continua Masnada, «coordinare tutte le attività di controllo senza il rischio di imbrigliare il business non deve essere stato facile. A ciò si aggiunga la necessità di programmare una seria attività di risk assesment, soprattutto per quelle aziende che gestiscono una grandissima quantità di dati rilevanti, e la successiva creazione di presidi di tutela contro la perdita e l'accesso non autorizzato di tali dati. Basti pensare che una statistica afferma che nel 2020 si stima che il costo sopportato dalle imprese a seguito degli attacchi informatici e dei data breach nel mondo dovrebbe ammontare a circa tre mila miliardi di dollari».

Secondo **Nadia Martini**, di Rödl & Partner Italy, «le nuove regole richiedono un importante cambio culturale: si è passati dal percepire la privacy come un adempimento burocratico e formale di mera compliance, che imponeva regole e soluzioni uguali per tutti, al percepire la protezione del dato come data protection e quindi un adempimento sostanziale, che impone a ciascuno di studiare la propria situazione, capire i rischi concreti e individuare le proprie soluzioni. Questo importante cambio di passo, ha comportato la necessità in tutte le aziende di revisionare tutti i processi e implementare controlli che prima non vi erano».

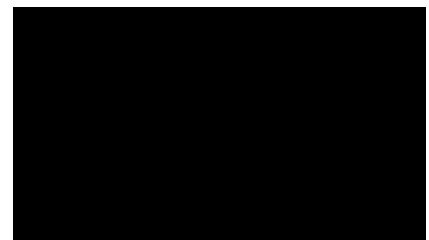
A parere di Luigi Fontanesi e Paola Furiosi, di Santa Maria studio legale associato, «i dati relativi ai primi quattro mesi dall'entrata in vigore del Regolamento europeo denotano un notevole aumento delle segnalazioni e dei reclami in materia di inosservanza della normativa (entrambi quasi raddoppiati) così come di casi di data breach. Ciò è attribuibile anche ad un incremento della consapevolezza degli interessati al trattamento dei dati personali sui diritti ad essi spettanti. La prima fase ispettiva da parte del nucleo specializzato per la privacy della Guardia di Finanza, da poco iniziata, riguarda i settori bancario e finanziario. Anche alla luce del nuovo principio della c.d. accountability, le imprese avranno modo di provare in maniera documentata di aver adottato tutte le misure necessarie per adeguarsi alla nuova disciplina, evitando onerose sanzioni economiche. Ricordiamo che possono ammontare, nell'importo più elevato, ad una cifra fino a 20 milioni di euro o corrispondente al 4% del fatturato complessivo dell'impresa».

Simona Gallo, partner di Jenny.Avvocati, sottolinea come «le difficoltà risiedono non solo nelle misure di sicurezza, sulle quali l'attenzione era già alta in passato, quanto nella gestione di eventuali databreach e delle procedure di conservazione dei dati, i cui tempi vanno comunicati agli interessati al momento della raccolta del dato. Il nuovo approccio risk-based al sistema privacy è sicuramente più ostico per le piccole imprese, specie se commerciali e, quindi, poco avvezze alla valutazione dei rischi in ambito sicurezza. Paradossalmente, però, sono queste le aziende più esposte a rischi privacy, perché gestiscono database di clienti per la vendita tramite e-commerce».

A parere di **Bridget Ellison** di De Berti Jacchia, «dal lato delle imprese, credo che la maggior parte



DIRETTA LE FONTI TV



NEWSLETTER

Iscriviti alla newsletter

Email: *

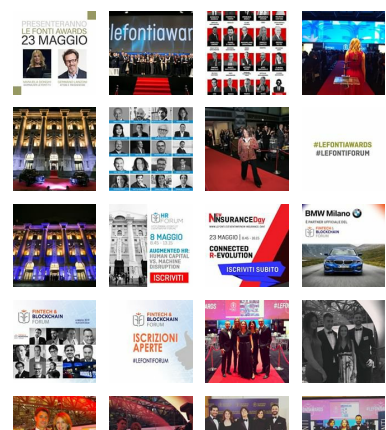
Nome: *

Cognome: *

Ho letto [l'informativa sulla privacy](#)

CONFERMA

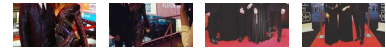
lefonti_group



delle società, in particolar modo quelle che beneficiano di una struttura sufficientemente ampia e complessa, abbiano preso sul serio il tema "privacy", facendo quanto necessario per conformarsi alla nuova normativa. La mia sensazione è che ormai sia pressoché terminata la fase di preparazione documentale, adeguamento dei processi aziendali e formazione delle società in ambito privacy, mentre stiamo per entrare in una fase in cui le società, fatti propri i principi della materia, dovranno utilizzare correttamente la documentazione e attenersi in concreto a quanto è stato pianificato per conformarsi al Gdpr. In pratica le società stanno passando dal processo di integrazione della privacy nei processi aziendali all'implementazione di tali processi e alla "privacy by default". «Come intuibile», continua Ellison, «conformarsi alle nuove regole è stato per le società più difficoltoso ove abbia implicato l'abbandono di alcune vecchie prassi ormai ampiamente consolidate, oppure, laddove abbia comportato la dilatazione delle tempistiche solitamente proprie di un processo aziendale, come, ad esempio, la selezione di un fornitore, che deve essere accompagnata da un'attenta valutazione degli aspetti privacy. Altri aspetti critici sono costituiti dalla necessità per l'impresa di essere in grado di reperire nelle proprie banche dati tutti i dati personali di un determinato soggetto in tempi abbastanza rapidi in caso di esercizio dei diritti di accesso, di cancellazione o di portabilità e dalla determinazione dei tempi di conservazione dei dati e della loro cancellazione; in passato, di fatto, molte società conservavano i dati personali senza limiti di tempo».

Secondo **Jacopo Destri** di C-Lex, «è certamente aumentato il livello generale di consapevolezza e sensibilità in relazione alle tematiche legate alla privacy e alla protezione dei dati personali. Tuttavia, ritengo che ancora oggi molti operatori, soprattutto quelli medio-piccoli, siano in ritardo e non abbiano completato appieno il processo di adeguamento rispetto al nuovo assetto normativo. Il principio di accountability introdotto dal regolamento presuppone una forte sensibilità che inevitabilmente richiede un periodo di maturazione più ampio. Va evidenziato inoltre che l'adeguamento alla normativa viene ancora percepito da parte di molti come un adempimento di carattere statico e non come un fattore che deve necessariamente divenire parte integrante dei processi aziendali nel rispetto dei principi di privacy by design e by default. Ritengo pertanto che ci vorrà ancora del tempo per una piena integrazione della protezione dei dati personali nei processi, anche decisionali, di tutti gli operatori. Si tratta in ogni caso di un percorso fisiologico che, in virtù della portata generale della normativa, deve necessariamente passare attraverso l'attività di indirizzo rimessa all'opera insostituibile delle Autorità di controllo e del nuovo comitato europeo per la protezione dei dati». «Le maggiori difficoltà», continua Destri, «si riscontrano nell'implementazione concreta della normativa. Infatti, il regolamento e le norme di attuazione fissano principi di carattere generale che rimettono agli operatori economici valutare nel caso specifico modalità di attuazione che garantiscano un livello adeguato di protezione dei dati personali. Ad esempio, il regolamento, nell'ambito delle nomine di responsabili e sub-responsabili esterni prevede un approccio di natura gerarchico che non rende sempre agevole gestire filiere complesse di fornitura ovvero quelle in cui il rapporto con il titolare è sbilanciato in favore del responsabile esterno. Tali situazioni si complicano ancor di più in ambito digital, in relazione al quale si attende con fiducia il regolamento e-privacy, con l'auspicio che questo semplifichi e tenga conto di alcune specificità del settore. Inoltre, sotto diverso profilo, considerato il margine di discrezionalità accordato dal regolamento ed i numerosi margini di incertezza interpretativa che ancora oggi permangono, non è infrequente imbattersi in scelte la cui tenuta di fronte ad eventuali accertamenti è assai dubbia».

Francesco Falco di DWF afferma che «tra le principali difficoltà nell'implementazione del Gdpr da parte dei soggetti che operano nel mondo finanziario, vi è quella del coordinamento tra il Gdpr e le molteplici normative di settore che già regolano il mondo della finanza. A prescindere, infatti, dall'interrelazione tra normative distinte, il rischio, sotto un profilo di governance/compliance, è quello di appesantire eccessivamente le strutture ovvero di non riuscire ad armonizzare le procedure interne rispetto ai diversi settori di intervento, che pure potrebbero condividere ambiti applicativi. A ciò occorre aggiungere che la tutela dei dati, genericamente intesa, è sempre più attenzionata dal legislatore e che, pertanto, le normative che potrebbero andarsi ad accavallare potrebbero crescere



Carica di più...

Seguire Instagram

EDITORIALE



Studi legali, serve trasparenza

Studi legali alla sfida della trasparenza. A pretendere dagli avvocati maggiore chiarezza sui costi derivanti...



I PIÙ LETTI



Chi ha fatto più affari nel 2018



Studi legali, serve trasparenza



MJ Hudson Alma apre a Milano

SEGUICI SU

Seguici su Facebook

Seguici su Twitter

Seguici su YouTube

Seguici su LinkedIn

rapidamente di numero». «Per le realtà di maggiori dimensioni», continua Falco, «l'implementazione del Gdpr appare come una sfida da vincere nel contesto della competizione tra imprese, per rafforzare la fiducia dei propri stakeholders. Nelle imprese più piccole, invece, l'implementazione del Gdpr non collima con l'idea di fornire ulteriore valore aggiunto, ma sembra più atteggiarsi ad un'ulteriore burocratizzazione dell'attività. In altri termini, il Gdpr è vissuto, per le grandi imprese, come un'opportunità di crescita e sviluppo, mentre per le piccole imprese, come fonte di costi e impacci. Per tale ragione, mentre le grandi imprese hanno dedicato risorse e capacità nell'attuazione del regolamento, le piccole realtà faticano ad interessarsi all'attuazione del regolamento».

A parere di **Giulio Graziani** di Elexia «le imprese e i soggetti operanti nel mondo finanziario avevano ante Gdpr un sistema di compliance che necessariamente imponeva una certa attenzione alla privacy. Credo quindi che sicuramente sia stato affrontato un lavoro di adeguamento che però potrebbe essere stato agevolato dal sistema privacy già implementato». Rispetto all'attività di verifica e sanzione da parte del Garante, secondo Graziani «non vi sarà un aumento delle verifiche, è più probabile che si possa assistere a un incremento del valore delle potenziali sanzioni comminate, con un conseguente livello di attenzione maggiore da parte delle imprese che, auspichiamo, possano attivarsi per ribaltare la percentuale di coloro che non sono ancora a norma».

Gianluigi Marino di Osborne Clarke ritiene che «le maggiori criticità sono quelle relative alla sovrapposizione tra le norme del Gdpr e della normativa e-privacy nonché al pieno sfruttamento delle opportunità date dalla PSD2. Inoltre, non è sempre facile individuare correttamente la base giuridica adatta a singoli trattamenti di dati personali. Anche il pieno e tempestivo riscontro alle richieste di esercizio dei diritti degli utenti trova talvolta difficoltà tecniche e organizzative». «Il Garante», continua Marino, «utilizzerà tutti gli strumenti a sua disposizione: dagli ammonimenti alle sanzioni pecuniarie. L'autorità si sta concentrando sui "grandi data controller" come gli istituti bancari, le telco e, in generale, chi tratta grandi database per finalità di marketing. Prevedo che si inizieranno ad avere i primi punti di riferimento quanto alla concreta applicazione dei criteri previsti dal Gdpr per l'irrogazione delle tanto temute sanzioni pecuniarie e, soprattutto, al giudizio dell'autorità quanto alle valutazioni interne svolte in relazione all'utilizzo della base giuridica del legittimo interesse. Fino all'avvento del Gdpr, infatti, il legittimo interesse era una base giuridica valida solo nella misura in cui fosse approvata dal Garante tramite provvedimenti generali o specifici. Ora invece è rimessa alla responsabilità del singolo titolare del trattamento che deve autovalutare la legittimità del ricorso a tale base giuridica».

Lucia Bressan dello studio legale Bressan osserva che «le piccole imprese hanno tuttora difficoltà a cambiare prospettiva e passare da un approccio esecutivo incentrato sull'adempimento formale ad un approccio responsabile che mette al centro il dato personale, e dunque la persona anziché il prodotto. Ancora sono molte le imprese che hanno adottato soluzioni di sola facciata, senza affrontare correttamente il processo di adeguamento. Inoltre solo con grande fatica, e in numero ancora limitato, le imprese hanno compreso quanto fosse importante cogliere l'occasione per rivedere procedure e processi aziendali, strutture organizzative in essere e dunque in tal modo lavorare anche sulla organizzazione efficiente ed ottimale. In questo senso la privacy compliance costituisce un valore aggiunto, grazie alla multidisciplinarietà che la materia impone, modificando la cultura d'impresa. Dal punto di vista pratico, nelle grandi imprese hanno trovato impatto in particolare le novità introdotte dal Gdpr ovvero le valutazioni d'impatto e la messa in atto dei nuovi approcci, oltre alla figura del Dpo e la corretta qualificazione e collocazione di quest'ultimo all'interno dell'azienda. Tutte le imprese si sono particolarmente spese sulla gestione dei fornitori (outsoucer) di servizi». «Sta terminando il periodo "soft", di tranquillità», conclude Bressan, «ma da giugno assisteremo alla implementazione di severi provvedimenti pronunciati soprattutto contro quelle imprese e quegli enti che non si sono adeguate ovvero hanno continuato ad affrontare con leggerezza il tema della protezione sostanziale dei dati, ovvero, ancora, hanno adottato soluzioni di sola facciata».

Mascia Cassella, di MBC Lex, afferma che «molte imprese si stanno adeguando alla nuova normativa, sia quelle che già erano compliant con il codice privacy del 2003, sia quelle che hanno risentito dell'eco mediatico del nuovo regolamento. Stiamo assistendo un grande numero di aziende dedicandoci non solo alla predisposizione della documentazione necessaria, ma anche alla formazione che teniamo in loco alla presenza di tutto il personale e che ci sta dando un ottimo riscontro in termini di interesse e di occasione per riunire il personale».

Rosanna Sovani di LSCube studio legale ritiene che «una prima criticità è senz'altro quella legata ai tempi di conservazione dei dati personali. Se da un lato, infatti, è corretto che dati personali non più necessari siano cancellati o anonimizzati, dall'altro le imprese che operano in settori fortemente regolamentati e sotto stretta vigilanza delle autorità competenti, come quelle del settore finanziario e assicurativo, hanno una certa ritrosia a cancellare dati personali per il timore che potrebbero essere loro richiesti in un momento successivo proprio da quelle autorità alla cui vigilanza esse sono soggette. Il problema nasce dal fatto che, in Italia, si ha una carenza di normative specifiche di settore che indichino in modo certo e chiaro quali siano i tempi di conservazione oltre i quali non sarà più possibile richiedere alle imprese di fornire informazioni e dati riferiti a persone fisiche identificate o identificabili. Sotto tale aspetto, pertanto, sarebbero necessari interventi normativi che permettano alle aziende di cancellare i dati personali non più necessari senza il timore di rimanere scoperte in caso di future richieste da parte delle autorità competenti. Una seconda criticità è quella dell'assolvimento dell'obbligo informativo nei confronti degli interessati. In ambito finanziario esiste spesso la necessità di condividere una grande mole di informazioni per prevenire, ad esempio, frodi e fenomeni come il riciclaggio di denaro. In questo contesto, spesso non è chiaro chi debba assolvere gli obblighi di informativa nei confronti degli interessati; anche in questo caso un intervento legislativo o un provvedimento chiarificatore dell'Autorità garante per la protezione dei dati personali avrebbero un impatto positivo».

Per **Rosamaria Bevante** dello studio ArlatiGhislandi, «la maggiore difficoltà nel processo di adeguamento al regolamento europeo è certamente quella di prevedere misure disposte a consolidamento della protezione dei dati senza che queste intacchino la redditività del business; ma ancor di più il fatto di dover accettare che i vari processi aziendali (già collaudati e funzionanti) debbano essere ora sottoposti a un censimento ex novo che comporti valutazioni di integrità e, a volte, di veri e propri interventi strutturali».

I penalisti

Armando Simbari di DFS rileva come «un aspetto critico è rappresentato dalla necessità di un costante aggiornamento del sistema di gestione del trattamento dei dati; è diffusa la convinzione che l'adeguamento al Gdpr sia un adempimento da assolvere una tantum. Invece, è necessario che le imprese, soprattutto nel caso di realtà aziendali complesse, predispongano strutture e personale in grado di verificare regolarmente l'adeguatezza del sistema e di adeguarlo costantemente ai cambiamenti che abbiano un impatto sulla privacy. Un'altra problematica attiene alle risorse economiche destinate all'adeguamento al decreto: se è vero, come si è detto, che la maggior parte delle imprese ha stanziato un budget dedicato, è anche vero che, soprattutto nell'ambito delle piccole realtà, esso risulta spesso insufficiente a garantire una corretta gestione del trattamento. Lo stanziamento di risorse inadeguate rappresenta un rischio elevato per le imprese se si considera che il decreto prevede sanzioni molto severe, non solo amministrative ma anche penali. A questo proposito, è importante sottolineare che il d.lgs. n. 101 del 2018, che ha recentemente modificato la sezione del Codice della privacy dedicata alle sanzioni, ha implementato il numero e la tipologia dei reati connessi al trattamento dei dati. Per esempio, con il nuovo art. 167-bis è stata introdotta la fattispecie di comunicazione e diffusione di dati personali trattati "su larga scala" in violazione di certi requisiti normativi, tra cui il consenso dell'interessato laddove richiesto. La fattispecie in questione ha mutuato il concetto di "archivio" automatizzato dal nuovo Gdpr, che con tale

espressione intende "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico". Altra fattispecie di nuovo conio è quella introdotta dall'art. 167-ter del Codice della Privacy, che punisce in modo ugualmente grave, fino a quattro anni di reclusione, l'acquisizione fraudolenta dei dati personali oggetto di trattamento su larga scala. Si deve segnalare che, per evitare che la reazione sanzionatoria risulti eccessiva rispetto all'offesa, il legislatore ha ritenuto di prevedere, relativamente ai predetti reati, una diminuzione della pena nel caso in cui venga applicata, per gli stessi fatti, anche una sanzione amministrativa. Infine, oltre a confermare la fattispecie di false dichiarazioni al Garante, il nuovo Codice ha introdotto altresì quella di interruzione di un procedimento davanti alla medesima autorità e quella di inosservanza dei provvedimenti da essa adottati».

A parere di **Fabio Cagnola** di Cagnola & associati «tra le maggiori criticità che le imprese di tutte le dimensioni hanno riscontrato vi sono innanzitutto quelle legate alla raccolta e alla mappatura dei dati personali. In particolare, si sono riscontrate difficoltà legate all'adeguamento ai requisiti tecnico-informatici, necessari ad esempio per cifrare e anonimizzare i dati. Infine, si segnalano problematiche legate banalmente agli scarsi investimenti, alla carenza di sensibilizzazione dei dipendenti o alla incomprendenza della normativa. Il mancato rispetto della normativa ha ovviamente conseguenze negative che vanno dalla imposizione di misure correttive alla irrogazione di sanzioni amministrative pecuniarie. Alcune gravi violazioni danno luogo anche a responsabilità penale. Si pensi ad esempio all'art. 167 del Codice della Privacy, il quale punisce violazioni legate al trattamento dei dati personali, qualora poste in essere con la finalità di profitto o di arrecare un danno all'interessato, oppure all'art. 168, il quale punisce chiunque produca documenti falsi oppure dichiarare il falso innanzi al Garante nel corso di accertamenti o in un procedimento».

I general counsel

Umberto Simonelli, chief legal & corporate affairs officer di Brembo, che ha avviato l'attività di assessment e adeguamento al Gdpr circa un anno e mezzo prima dell'entrata in vigore del regolamento, afferma che «una prima difficoltà che abbiamo riscontrato nella fase iniziale di assessment aziendale delle attività è stato far comprendere ai nostri interlocutori il concetto di dato personale ed il concetto di trattamento, al fine di recuperare le necessarie informazioni per mappare adeguatamente tutti i trattamenti aziendali e quindi completare il Registro delle attività di trattamento. Altre complessità le abbiamo riscontrate nell'individuazione dei fornitori che devono essere nominati Responsabili ai sensi dell'articolo 28 del Gdpr. Infatti non sempre è facile classificare un fornitore come titolare autonomo o responsabile in quanto per alcuni servizi ricevuti non è così chiaro chi stabilisce la finalità, i mezzi e la modalità del trattamento. Inoltre mentre in alcuni casi la negoziazione dell'accordo di nomina a Responsabile è stata snella e veloce, in altri casi, con alcuni responsabili, ha richiesto tempi più lunghi. Un'altra attività complessa è connessa al concetto di accountability, ossia la rendicontazione della compliance alla normativa del Gdpr. Pertanto è essenziale tenere traccia e rendere conto di tutte le scelte aziendali fatte e non fatte e del ragionamento alla base di tali scelte».

Stefano Brogelli, legal and compliance director di Axpo, che ha adottato un modello organizzativo per il trattamento dei dati rivedendo le precedenti policy e procedure in materia di trattamento dei dati, sottolinea che «la predisposizione del modello e l'attuazione delle regole ivi previste nell'attività di tutti i giorni ha comportato e continua a comportare un non trascurabile sforzo da parte delle diverse funzioni aziendali, in particolare di quelle più direttamente interessate, come la funzione Ict e l'area commerciale. Per ottenere il necessario coinvolgimento dei colleghi è stato inizialmente necessario diffondere consapevolezza circa l'importanza di adeguarsi alla nuova normativa. Ciò ha reso possibile ottenere la fattiva collaborazione di tutti, anche di chi inizialmente non aveva idea di cosa l'acronimo Gdpr significasse». «La società», continua Brogelli, «ha valutato di affidare l'incarico

di Dpo ad un soggetto esterno per motivi organizzativi. La funzione legal & compliance è comunque il principale punto di riferimento all'interno dell'azienda per ogni questione attinente al trattamento dei dati e collabora costantemente con il Dpo per assicurare il rispetto del modello organizzativo».

AVVOCATI

GDPR

GENERAL COUNSEL

PENALISTI

PRIVACY



Autore **REDAZIONE** – 23 Maggio 2019

[← ARTICOLO PRECEDENTE](#)

Studi legali, serve trasparenza

[PROSSIMO ARTICOLO >](#)

I general counsel chiedono agli avvocati più chiarezza sulle tariffe

POST CORRELATI



I general counsel chiedono agli avvocati più chiarezza sulle tariffe



Studi legali, serve trasparenza



Avvocati, in dieci anni bruciati 20 mila euro di reddito

Comments are closed.

LE FONTI LEGAL



CONTATTI

Le Fonti s.r.l.
Via Dante, 4 - 20121 Milan - Italy
Tel: 0039 02 873 863 06
info@lefonti.it

PEC: editricelefonti.it@pec.it

LINK UTILI

[RANKING](#)
[MERCATO LEGALE](#)
[INTERVISTE](#)
[TAVOLE ROTONDE](#)

[Sign up](#)
Per la tua pubblicità

Informativa



Questo sito o gli strumenti terzi da questo utilizzati si avvalgono di cookie necessari al funzionamento ed utili alle finalità illustrate nella cookie policy. Se vuoi saperne di più o negare il consenso a tutti o ad alcuni cookie, consulta la [cookie policy](#).
Chiudendo questo banner, scorrendo questa pagina, cliccando su un link o proseguendo la navigazione in altra maniera, acconsenti all'uso dei cookie.