GDPR (General Data Protection Regulation)

in chiave HR :

Quale impatto sulla gestione dei dati delle

Risorse Umane

14 Giugno 2018 ANDRIOLI- MAYERSON & PARTNERS

- **COS'E' IL GDPR (2016/679/UE)?**

  E' Il **REGOLAMENTO EUROPEO SULLA TUTELA DEI DATI PERSONALI** (GDPR) ovvero la nuova legge sulla privacy, entrato in vigore il 25 maggio 2018 e promette di introdurre una nuova era di governance dei **dati** e dei **requisiti avanzati in materia di sicurezza e trattamento dei dati personali** in un ottica di **trasparenza, semplificazione e unificazione** tra Paesi UE.

- **OBBIETTIVO** del GDPR :

  > E' PROTEGGERE i cittadini europei **quando** i loro dati personali vengono elaborati, garantendone la SICUREZZA e PROTEZIONE

  > EVITARE USI IMPROPRI.

  Approvato dal Parlamento Europeo in aprile 2016, questo strumento **intende RAFFORZARE** e **UNIFICARE** la protezione dei dati personali **ENTRO I CONFINI** dell'UE; e *nasce* con l'obiettivo di ***migliorare le garanzie*** *per i cittadini e* ***MODIFICARE L'APPROCCIO DELLE AZIENDE*** *nei confronti del* ***TRATTAMENTO DEI DATI personali*** *DEI DIPENDENTI, garantendo un maggiore equilibrio tra aziende e individui.*

  Constatato *l'incremento esponenziale degli attacchi hacker* che minacciano di continuo la compromissione di milioni di dati sensibili in tutto il mondo, il GDPR **VUOLE STABILIRE** una **GUIDA UFFICIALE** per il **TRATTAMENTO, l' ARCHIVIAZIONE e l' UTILIZZO** dei dati del personale, **PREVENENDONE** la **PERDITA** e **IMPEDENDONE** la **CONDIVISIONE NON AUTORIZZATA,** *soprattutto* **NEL CASO** di trattamento interamente o parzialmente **AUTOMATIZZATO.**

GDPR: le principali novità

Nell'aprile 2016, è stato approvato dal Parlamento europeo il Regolamento n° 2016/679, il cosiddetto GDPR, **che in Italia ABOLISCE il «Codice in materia di protezione dei dati personali (c.d. Codice Privacy 196/2003).**

Questo strumento legislativo è *self-executing*, ovvero **VINCOLANTE e DIRETTAMENTE APPLICABILE** in TUTTA Europa in base al Trattato sul Funzionamento dell'U E.

Si è scelta questa strada **per superare i limiti della precedente Direttiva,** che è stata **applicata in modi differenti in base alle diverse disposizioni dei singoli Paesi membri. È importante far notare che il GDPR è un Regolamento, non una Direttiva, il che significa che si applicherà allo stesso modo in tutti i 28 Stati membri senza richiedere un'implementazione nelle varie legislazioni nazionali**.

In seguito ad una maggiore globalizzazione, **al progresso delle tecnologie,** dei servizi digitali, **allo sviluppo di internet**, e all'evoluzione **dei concetti di privacy e protezione dei dati personali si è reso necessario emanare nuove norme in materia di protezione dati.**

L'**ADOZIONE** del GDPR **SERVE A RENDERE PIU' SOLIDA**, **semplice, coerente la struttura** NORMATIVA *relativa alla protezione dati personali* oltre che per favorire lo sviluppo del digitale all'interno dell'UE.

Per far ciò, è stata prevista l'*applicazione delle norme comunitarie anche a tutte quelle società che sono all'estero ma che operano nel mercato europeo che trattano dati personali dei cittadini/dipendenti dell'UE e che offrono beni/servizi a soggetti residenti nell'UE* o ne osservano il comportamento .

- Viene meno il requisito dell'autorizzazione nazionale a trasferite dati personali all'estero. Ciò significa che il **trasferimento** verso un paese terzo "ADEGUATO", potrà avvenire senza attendere l'autorizzazione nazionale del Garante. Tuttavia, *l'autorizzazione* del Garante sarà ancora *necessaria se un titolare desidera utilizzare clausole contrattuali ad hoc*.

- Il GDPR consente di ricorrere, nelle transazioni con paesi terzi, a codici di condotta ovvero a schemi di certificazioni per dimostrare che ha adottato "garanzie adeguate"

- Il GDPR vieta trasferimenti di dati verso titolari in Paese terzo *sulla base di decisioni* giudiziarie o ordinanze amministrative emesse da autorità di tale Paese Terzo, a meno dell'esistenza di accordi internazionali di mutua assistenza giudiziaria o accordi di analoga natura.

- Il GDPR chiarisce che possono essere trasferiti i dati verso un Paese terzo "non adeguato" se sussistono importanti motivi di interesse pubblico *riconosciuto dal diritto dello Stato membro chiamato a trasferire e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente*

GDPR E AZIENDA

Il PRIMO OBBIETTIVO è stato quello di *far comprendere* alle aziende ***il cambiamento di approccio al tema privacy*****:** IL GDPR, (**Regolamento europeo sulla tutela dei dati personali)**, **obbliga** ad una **RAZIONALIZZAZIONE** dei flussi di dati **INTERNI all'azienda, rispetto ai dipendenti, ed ESTERNI rispetto ai fornitori.**

Le premesse

Si tratta di una manovra economica messa in atto dall'Europa, non solo in termini di **protezione del know how**, ma anche nel **guidare le scelte aziendali in merito ai fornitori**, soprattutto per accordi su prodotti o servizi che incidono su investimenti pluriennali.

Nel periodo di passaggio, ovvero i due (2016/2018) anni concessi alle imprese per allinearsi al nuovo assetto, i **Provvedimenti del Garante** hanno continuato a essere **considerati punto di riferimento, non derogabile,** per la corretta gestione della materia, oltre **a *rappresentare un'utile guida per prepararsi all'evoluzione in atto.***

Si è iniziato con il **DELIMITARE** l'ambito di **APPLICAZIONE** del GDPR

Esso riguarda, come abbiamo detto precedentemente, **TUTTO il TERRITORIO EUROPEO, ma TRAVALICA I CONFINI** quando si parla di **ONERI DI GESTIONE DEL RAPPORTO CON I FORNITORI,** che esternalizzano delle attività al di fuori dell'UE, **TRATTANDO DATI PERSONALI DI CITTADINI EUROPEI, DOVRANNO GARANTIRE GLI STANDARD PREVISTI DALLA NORMATIVA COMUNITARIA.**

Rispetto all'ambito sostanziale, il regolamento si applicherà sempre dove sarà realizzato un trattamento di dato personale. In tal senso devono essere consideratati anche Nick name e dati di business intelligence che diventano funzionali alle attività aziendali.

LE AZIONI MESSE IN CAMPO DALLE AZIENDE:

In vista dell'applicazione del GDPR, le aziende multinazionali si sono organizzate per ***mettere al sicuro*** :

- il **PROPRIO SISTEMA INFORMATIVO**;
- il **FLUSSO DEI DATI IN ENTRATA e IN USCITA**.

A CHI ATTRIBUIRE LE FUNZIONI della responsabilità *a* tradurre la consapevolezza della sicurezza dei dati al resto dell'organizzazione.?A primo impatto

Il Rischio è farle ricadere :
- IT MANAGER in un'ottica tecnica
- **agli uffici legali**

In quanto ci sono delle considerazioni oggettive nel nuovo quadro giuridico che hanno impatti trasversali:

- **Primo:** il GDPR accresce il diritto per gli individui;
- **Secondo:** rafforza gli obblighi in capo alle imprese;
- **Terzo:** accresce le sanzioni economiche in caso di inadempienza fino a 20 mln o al 4% del fatturato globale.

Inoltre, ha un **impatto su tutti i settori** di business e, per questo, **RIGUARDERA'QUALUNQUE AZIENDA CHE ABBIA DIPENDENTI**, anche quando non gestisce e non coinvolge dati di consumatori.

Dunque, **gli IMPATTI del nuovo regolamento si riversano** nella GESTIONE **dei flussi di dati dei dipendenti con una serie di regole a cui gli uffici delle risorse umane- ufficio del personale (HR)** dovranno prestare attenzione e/o ripensare al loro approccio.

L'**ampiezza e generalità** del GDPR rendono indispensabile una breve **RILETTURA dei principali temi privacy** in funzione delle competenze degli HR Manager:

1. **La privacy dei dipendenti:** il tecno controllo è il primo argomento a cui prestare attenzione per non intaccare la tutela della privacy del lavoratore.

Dal concetto del "**controllo a distanza**" (utilizzo di telecamere, di strumenti di geolocalizzazione il potere di controllo del datore di lavoro **è stato ampliato** dall'evoluzione tecnologica). Ma oltre alla reperibilità geografica, i dati di navigazione in internet, l'uso delle mail etc., l'ufficio HR è a conoscenza di molte altre informazioni dei dipendenti, spesso anche sensibili: situazioni familiari, malattie, iscrizioni a sindacati, solo per citare qualche esempio.

2. **L'importanza dei consensi**:

molte aziende attivano il trattamento dei dati sulla base dei consensi dei dipendenti rilasciati **in sede di firma di contratto** di lavoro. Con l'entrata in vigore del GDPR, il titolare **deve dimostrare** che l'interessato **ha espresso** il proprio consenso **liberamente** *e può esercitare il diritto di revocarlo in qualsiasi momento*. La richiesta di consenso deve essere data in modo **chiaramente distinguibile** dalle altre materie, **in forma comprensibile e inequivocabile**. Il trattamento di *dati particolari/ sensibili* (come ad esempio l'appartenenza sindacale o i dati genetici o biometrici) è lecito solo se c'è:

a) un **consenso esplicito**

b) nel caso in cui questi dati **siano necessari ad assolvere obblighi in materia di diritto del lavoro.**

3) **Rafforzamento dei diritti dei dipendenti:**

gli interessati del trattamento (per gli uffici HR tutti i dipendenti) **vedono aumentare** i loro diritti.

> Innanzitutto, devono poter **accedere a dettagliate informazioni** sul flusso dei loro dati, perché e come vengono trattati, sottolineando la trasparenza e la sicurezza negli utilizzi.

> In secondo luogo, possono chiedere la **rettifica o la cancellazione** di dati non più necessari, applicando il cosiddetto **diritto all'oblio**. Si pensi alla conclusione di un rapporto di lavoro e alla dismissione di tutti gli account e strumenti contenenti i dati dell'ex-dipendente.

4) **I rapporti con i fornitori:**

Non si deve dimenticare che la normativa si applica anche a tutti i fornitori (HR service providers) **che gestiscono i dati dei dipendenti per conto dell'azienda**. **Si tratta di tutti i software di gestione del personale**, prodotti di Business Intelligence, sistemi di apprendimento e sviluppo (L&D: Learning and Development), basati **su tecnologie cloud, che** dovranno **rendere evidenza dei flussi d'informazione** specialmente nelle organizzazioni internazionali che impongono **dei trasferimenti di dati a piattaforme di Paesi terzi**. Inoltre, non vanno tralasciate : le

> Agenzie per il lavoro, > le società che svolgono recruiting,> i consulenti a vario titolo che ruotano attorno ai dati dei dipendenti, che pure costituiscono un tassello nel workflow degli Uffici HR.

Ad esempio: La maggior parte dei sistemi di **e-learning**, per esempio, si avvale di contratti Cloud che permettono un utilizzo da qualsiasi posto, in qualsiasi strumento e in qualsiasi orario. Questo complica di molto la tutela dei dati dei dipendenti, soprattutto se poi il lavoratore utilizza il proprio device (BYOD).

I fornitori / subfornitori prescelti, secondo le regole del GDPR, devono garantire **di aver considerato tutti gli aspetti di sicurezza** dei dati e **compliance (conformità) normativa**. Per effetto dell'armonizzazione legislativa **sarà più agevole far circolare i dati dei dipendenti all'interno** delle imprese in **Europa**, ma sappiamo anche che il sistema di tutela varia totalmente dall'Europa agli USA o alla Cina, Paesi dove spesso le multinazionali hanno sedi e dipendenti.

Nonostante la complessità del GDPR, il tema della protezione dei dati non è nuovo ed il mercato degli HR service providers che ha già modificando i prodotti destinati ad un utilizzo globale in funzione delle stringenti regole europee. E' necessario però che gli HR Manager si avvicinino al GDPR per l'importanza di tutte le sfide che ne derivano **senza delegare ad altri uffici**, e al contempo **comprendano che ogni dato dei dipendenti *è un dato personale*, compresi quelli relativi allo sviluppo di carriera e all'apprendimento.**

5) **Organizzazione e misure di sicurezza:**

il GDPR prevede **una serie di adempimenti** in capo alle aziende per rafforzare l'effettività di queste regole.

> Dal **prevedere strumenti atti a valutare i rischi** dei dati trattati (Privacy Impact Assessment : **PIA**),

> all'**obbligo di notificare le violazioni** (data breaches).

Se la "breccia" del sistema informativo riguarda i dati dei dipendenti, il datore di lavoro deve darne immediata comunicazione agli interessati nel caso in cui ci sia rischio elevato di compromettere i loro diritti e libertà.

Pertanto, il **GDPR e** la designazione del **DPO** (Data Protection Officer) o **Responsabile della Protezione dei Dati Personali**, obbligatorio nelle realtà aziendali con più di 250 dipendenti, obbligano a **un ripensamento organizzativo proprio nell'ottica di mappare i flussi informativi in entrata ed in uscita.**

GDPR: cosa cambia per gli uffici HR e i dipendenti

Con l'introduzione della nuova normativa gli *uffici HR saranno i primi a esserne coinvolti* sia dal punto di vista **degli obblighi che delle conseguenze.** Il GDPR **innalza i** requisiti per la sicurezza delle attività di elaborazione dei dati personali che sono potenzialmente più a rischio.

Il GDPR richiede alle aziende di dettagliare:

- **quali sono le informazioni sui dipendenti,**
- **chi ha accesso alle informazioni** e..
- **dove risiede l'informazione**.

La mancata conformità ha come conseguenza, le multe ingenti. Nonostante questo, un'indagine ha riscontrato che le piccole e medie imprese e in generale l'impresa italiana, **non hanno** una **consapevolezza** generale dei requisiti della nuova normativa, **come prepararsi** a essa e **l'impatto che può avere la non conformità sulla sicurezza dei dati sui risultati aziendali**. Oltre l'80% sa poco o nulla in merito al GDPR.

Qualunque azienda faccia affari nell'Unione Europea gestendo i dati personali dei residenti/dipendenti dell'UE, indipendentemente dal fatto che l'azienda si trovi o meno in Europa, deve adeguarsi a quanto norma il GDPR .

Gli obiettivi principali della normativa:

> **sono armonizzare i principi di protezione dei dati personali in tutta l'UE e**

> **offrire alle persone un maggiore controllo sul modo in cui i propri dati vengono utilizzati**.

Si tratta davvero di dare ai dipendenti / cittadini ue una voce in più *su come le aziende raccolgono, archiviano e proteggono* i loro dati".

Pertanto è importante che **i datori di lavoro** non trascurino il GDPR e i notevoli cambiamenti che comporterà.

A livello aziendale, sarà soprattutto l'ufficio HR a essere impattato dalla nuova normativa: come e in che modo?

Innanzitutto è bene agire per punti :

- **In primo luogo** l'ufficio HR deve **analizzare e studiare** i nuovi requisiti richiesti dal GDPR e determinare **in che modo possono essere applicati** nell'azienda.

- **In secondo luogo**, occorre **rivedere i processi esistenti** e **MAPPARE** il **flusso dei dati che sono già in gestione;** *questo procedimento consente di individuare lacune che dovranno essere progressivamente colmate.*

- **In terzo luogo**, fatto ciò, è fondamentale **redigere un preciso piano di azione, coinvolgendo tutte** le parti interessate, il che significa probabilmente chiamare in causa chi nell'azienda si occupa di privacy, legale, HR, IT, Vendite e Marketing,…

Parte fondamentale di questo piano sarà quella ***di DOCUMENTARE e CONFERMARE il COMPLETAMENTO delle azioni stabilite****, per poi passare alla fase successiva.*

> ovvero la stesura/realizzazione di un buon **programma di governace** in quanto il GDPR *è incentrato* **sulla RESPONSABILITA'** e sulla **CAPACITA'** di **DIMOSTRARE** la **CONFORMITA'** su base **CONTINUATIVA**. Il ché significa che in qualsiasi momento, l'azienda deve dimostrare la conformità delle procedure adottate con i dettami del GDPR, poiché la legge concede molto potere alle autorità di regolamentazione di ciascuno Stato membro per controllare, indagare e potenzialmente applicare sanzioni severe"...

Diritti dei dipendenti, COSA DEVE SAPERE IL DIPENDENTE?

Aumentano i diritti dei dipendenti.

> Innanzitutto, **DIRITTO DI ACCESSO (art.15)** potranno accedere a dettagliate informazioni sul flusso dei loro dati (questo avviene a titolo gratuito ma spetta al titolare stabilire l'ammontare dell'eventuale contributo solo se si tratta di richiesta infondata o di n. copie si deve tenere conto dei costi amministrativi sostenuti), perché e come vengono trattati, **pretendendo** trasparenza e sicurezza.

> In secondo luogo, possono chiedere: > **la cancellazione (art.17)** di dati non più necessari senza ingiustificato ritardo e/o la rettifica (art.16);

> il d**iritto all'oblio (art.17)**. è espressione del diritto alla privacy relativo a vicende personali diffuse via web oramai desuete e/o sconosciute ai più. Si dovranno trovare quindi soluzioni tecniche che consentano la cancellazione automatica dei dati non solo sul singolo sistema aziendale, tramite il quale i dati sono stati raccolti, ma anche su tutti gli altri sistemi aziendali all'interno dei quali sono stati diffusi. Si pensi soprattutto alla conclusione di un rapporto di lavoro e alla dismissione di tutti gli account e strumenti contenenti i dati dell'ex-dipendente

> Tale diritto può essere esercitato anche dopo la revoca del trattamento.

> Può chiedere l'applicazione del **DIRITTO DI LIMITAZIONE DEL TRATTAMENTO** (ART.18) :

Si tratta di un diritto diverso e più esteso rispetto al “blocco” del trattamento: in particolare è **esercitabile:** **1)** in caso di violazione sulla licealità dei dati;

2) se chiede la rettifica dei dati o si oppone al loro trattamento;

Tale diritto **prevede** che il dato personale **sia “contrassegnato”** in attesa di approfondimenti ulteriori pertanto è opportuno che si preveda nei propri sistemi informativi (elettronici e cartacei) misure idonee a tale scopo.

- Il lavoratore può appellarsi al **DIRITTO ALLA PORTABILITA' DEI DATI**. (art.20)

  Tale DIRITTO NON SI APPLICA ai trattamenti NON AUTOMATIZZATI (quindi non si applica agli archivi cartacei o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare sono PORTABILI SOLO I DATI TRATTATI CON IL CONSENSO DELL'INTERESSATO O SULLA BASE DI UN CONTRATTO STIPULATO CON L'INTERESSATOE SOLO I DATI CHE SIANO STATI FORNITI DALL'INTERESSATO AL TITOLARE.

- Inoltre il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, pertanto si deve, da entrambi i titolari, adottare misure necessarie a produrre i dati richiesti in “**formati interoperabili**”

Avere IDEE CHIARE.... DA SUBITO

.Al di là del dato ovvio – nome, indirizzo, data di nascita, stato civile, fascia di reddito ecc. – il dipendente ha presso la propria azienda informazioni quali la storia salariale, le esigenze dietetiche, lo stato del visto, la patente e molto di più.

Il dipendente potrà quindi richiedere in ogni momento, ed esercitare il proprio **diritto all'oblio**, anche in merito a tutti i dati che riguardano:

> **Recruitment**: CV, moduli di candidatura, invii personali.

> **Payroll**: tutti i dati personali presenti suo libro paga

> Spese, viaggi, visite mediche: dichiarazioni di spesa, documenti di viaggio, informazioni mediche e dentistiche.

Cornerstone OnDemand e il GDPR, cosa cambia per le HR?

Indubbiamente il nuovo regolamento può spaventare, purtuttavia le aziende hanno avuto molto tempo (2 anni) per prepararsi, pena pesanti sanzioni una volta che il regolamento sarà entrato in vigore. L**'aspetto positivo è che in fin dei conti il GDPR richiede l'implementazione di buone pratiche per la gestione dei dati e aiuta a limitare o diminuire i rischi** sia in caso sia :

> di attacco informati e/o furto informatico

> **obbligando a migliorare la qualità dei dati** e di conseguenza il **valore degli stessi**.

Scopo del GDPR è

> proteggere i dipendenti, in quanto cittadini europei, quando i loro dati personali vengono elaborati,

> garantire la sicurezza;

> garantire la protezione

> garantire che non vengano utilizzati impropriamente.

Finora le aziende **hanno puntato essenzialmente a proteggere i dati dei loro clienti,** ma non bisogna dimenticare che l**e stesse regole devono essere applicate anche ai dati sui dipendenti, compresi quelli sui candidati.**

Cosa comporta tutto questo per le HR?

Quando il GDPR sarà entrato in vigore, le aziende potranno raccogliere dati personali sui candidati, ma **esclusivamente quelli strettamente necessari al processo di selezione.**

Le aziende dovranno **ricevere il consenso per tutti i dati che richiedono il permesso esplicito** da parte dei dipendenti (i quali potranno ritirarlo in qualunque momento) **e se un dipendente per qualunque ragione lascia l'azienda anche i suoi dati personali dovranno essere cancellati.**

Per ogni altro dato, le aziende dovranno **chiedere il CONSENSO ESPLICITO** e qualunque informazione fornita potrà **essere utilizzata esclusivamente per il motivo per cui è stata richiesta**. *Se la persona non viene assunta, tutte le informazioni dovranno essere cancellate*. Analogamente, ***tutti i dati raccolti e archiviati sui dipendenti esistenti dovranno essere funzionali alla gestione o al ruolo*** *del dipendente.*

Nelle aziende che trattano migliaia di data point, la compliance comporta una preparazione molto accurata. Dal momento che può sembrare un lavoro immane, si raccomanda alle aziende di **affrontare la compliance al GDPR, per la parte relativa ai dati dei dipendenti,** in **TRE** semplici passi. E' chiaro che nella maggior parte dei casi non si partirà da zero, molte aziende hanno già implementato precise policy di gestione dei dati.

Step 1: Privacy by design/ by default

Privacy by design significa essenzialmente prendere in considerazione i requisiti di protezione dei **dati già nelle fasi di progettazione dei sistemi e dei processi,** ovvero **consiste nell'adozione di misure tecnico-organizzative a protezione dei dati, minimizzando l'uso non autorizzato di questi** (privacy by default) e **consentendone l'accesso solo agli incaricati autorizzati.**. Per essere conformi al GDPR, è più semplice creare un nuovo sistema o processo *e progettarlo tenendo in considerazione i requisiti anziché adattarli successivamente.*

La centralità dei **Principi Privacy By Design e Default (** privacy per progettazione e impostazione predefinita)**,** introdotti nella riforma europea, sono fondamentali per regolare contratti ed accordi con terze parti.

Dato che spesso tali accordi sono sanciti a medio o lungo termine, sarà più che opportuno per le imprese revisionare i contratti in essere o meglio realizzandoli ex novo rispettando tali dettami.

Il consiglio è di **iniziare dai dati,** non dal processo, e d**ocumentare la giustificazione per questi data point.**

Quindi, **analizzate i processi** che hanno a che fare con i dati realmente necessari e **incorporate i** requisiti di privacy e i diritti dell'utente all'interno di tali processi.

L'operazione sarà più semplice se avete una immagine chiara di tutti i vostri dati. E' più efficiente **costruire e disegnare i processi attorno ai dati necessari** *anziché adattare vecchi processi* ai nuovi regolamenti. Questa *è anche un'ottima opportunità per fare pulizia, con l'effetto collaterale di poter dimostrare la compliance con il principio di minimizzazione dei dati.*

Step 2: La privacy impatta sull'analisi

Il concetto di privacy by design può comportare molto lavoro: da dove cominciare? **Effettuate un audit** (revisione) **del processo e dei dati** che raccogliete e del trattamento di questi, **quindi eseguite una gap analysis** (analisi degli scostamenti **) per capire dove siano i maggiori rischi.** Pertanto riferendosi alla materia contrattuale, è bene approcciare consapevolmente anche il Privacy Impact Assessment (valutazione dell'impatto sulla privacy) (PIA), ovvero uno strumento atto a tener conto degli impatti del trattamento sui diritti dell'interessato e a valutare i possibili rischi collegati. Implicazione che, ancora una volta, coinvolgeranno l'intera filiera dei fornitori.

Ad esempio, in caso di violazione del sistema quali insiemi di dati comporterebbe le peggiori conseguenze? I dati sulla formazione o quelli sui salari? Bisogna partire da qui.

Considerate inoltre i dati che possono essere raccolti **automaticamente in quanto sarete responsabili delle azioni risultanti tanto da un processo automatico quanto da quelli manuali.**

Un **audit** (revisione) **aiuterà a identificare tutti i punti di debolezza e le aree di rischio**, . E' importante continuare a effettuare questi audit (revisioni) **regolarmente** per garantire la qualità e la compliance dei processi, oltre che per adattarli a future modifiche delle normative.

Step 3: Definire le responsabilità (= accountability)

Il terzo passo è la chiusura del cerchio. **Le aziende devono garantire trasparenza totale, anche riguardo a dove i dati dei dipendenti sono archiviati e come sono processati, chiarendo chi è abilitato ad accedere a questi dati**. il tutto dovrà essere documentato per dimostrare il grado di compliance(conformità). Questo è quello che viene definito **principio di responsabilità,** che essenzialmente si traduce nel documentare i data set (e *come questi sono conformi al principio di minimizzazione*), e nel documentare i processi (e *come questi implementano i principi della privacy e permettono agli utenti di esercitare i loro diritti*).

Step 3 e mezzo: Chi deve fare tutto ciò?

Molte aziende hanno scelto di nominare un responsabile generale della sicurezza dei dati che ***dovrà lavorare con tutti i dipartimenti***. Oggi, vediamo emergere una nuova figura **DPO** anche all'interno delle HR. E' nell'interesse delle HR avere uno specialista della protezione dei dati al proprio interno, che lavori a stretto contatto con il responsabile generale per garantire la compliance (conformità). *Gestire la riservatezza dei dati richiede conoscenze* legali, tecniche e di business e una figura che riunisca queste competenze dovrebbe garantire la conoscenza tanto delle normative locali quanto dei processi HR dell'azienda.

Il GDPR non è una normativa semplice ed è importante che le HR si siano preparati per tempo.

Il GDPR impone di ripensare > ai processi > alle modalità di trattamento e archiviazione dei dati personali.

Anche applicando i tre passi appena descritti, mettere in moto il processo può essere complicato. Tuttavia, lo sforzo sarà ripagato **dalla maggiore qualità** dei dati, **dalla maggiore efficienza dei processi e dalla diminuzione dei rischi di sanzioni**, oltre che da una migliore immagine dell'azienda e dalla maggiore motivazione dei dipendenti. .

La compliance (conformità) è un processo e la protezione dei dati una cultura: una volta realizzata si rivelerà uno strumento estremamente potente ed efficace

Pertanto è fondamentale che le aziende abbiano **identificato**, in questi 2 anni, **le modalità per adeguarsi alla nuova normativa, evitando così di arrivare impreparate** ad affrontare quello che viene considerato uno dei cambiamenti più significativi della storia della protezione dei dati.

Riassumiamo le principali novità per le aziende e le nuove figure di riferimento

> Titolare del trattamento: è la persona fisica o giuridica che determina le finalità i mezzi del trattamento dei dati personali;

> Contitolare del trattamento : sia ha quando un determinato trattamento sia effettuato da più titolari

> Nomina del RESPONSABILE DEL TRATTAMENTO ESTERNO ALL'AZIENDA (=Data Processor) che deve :

1) prestare garanzie sufficienti per mettere in atto misure tecniche ed organizzative per assicurare il rispetto dei requisiti imposti dal GDPR;

2) essere nominato con un contratto che contenga la descrizione dettagliata dei trattamenti di dati oggetto della nomina; deve inoltre disciplinare, nei termini previsti dal GDPR, gli obblighi del nominato in relazione alla protezione dei dati e alla loro sicurezza

> Persone autorizzate: incaricato del trattamento

> Nomina del DPO (Data Protection Officer), quale responsabile della protezione dei dati personali (dipendenti, partner, clienti, pubblico);

> Amministratore di sistema : è persona, in ambito informatico, finalizzata alla gestione e manutenzione dell'impianto di elaborazione , quindi ha il compito di predisporre le misure di sicurezza idonee a garantire la sicurezza e l'integrità dei dati trattati.

> Stop al silenzio assenso: tutte le aziende dovranno richiedere – ed essere in grado di documentare - in modo chiaro e inequivocabile il consenso dei dipendenti all'utilizzo dei propri dati da parte dell'azienda;

> Obbligo di introdurre valutazioni di impatto del rischio privacy;

> **Obbligo di notifica in caso di violazione dei dati** entro 72 ore all'autorità garante della privacy

> Introduzione di **sanzioni** più o meno gravi - fino al 4% del fatturato annuo globale dell'azienda, per un massimo di 20 milioni di euro - in caso di non conformità a quanto disposto dal Regolamento.

La figura del Responsabile della Protezione di dati (Data Protection Officer) o DPO

Il principale cambiamento organizzativo introdotto dal GDPR è **l'istituzione della figura del DPO - Responsabile della Protezione dei Dati**, che in molte aziende ancora non esiste.

In realtà, l'introduzione di questa funzione non è obbligatoria: il GDPR stabilisce la regola generale secondo cui "*Il DPO **è obbligatorio** solo se **l'attività principale** dell'azienda consiste nel **monitoraggio continuo e sistematico degli individui effettuato su LARGA scala,** oppure se vengono trattati su larga scala dati sensibili o i precedenti penali*". Spetta dunque alle aziende decidere in base al proprio specifico contesto di attività.

Tuttavia, data la complessità delle mansioni, la costante evoluzione dello scenario, l'aumento degli episodi di cyber-crimine e la portata delle sanzioni, le raccomandazioni vanno in direzione della nomina di questa figura così specifica e specializzata, che dovrà riportare ai livelli più alti del management- a meno che non si tratti di aziende che hanno a che fare con quantità di dati personali davvero modeste (ad esempio, il produttore di parti di ricambio per l'industria automobilistica potrebbe non necessitare di un DPO se ha solo clienti B2B).

IL DPO è chiamato a **fornire linee guida su tutte le questioni relative a tutte le attività di trattamento di dati personali in modo da garantirne la compliance** (conformità).

Il DPO dovrebbe essere ***coinvolto in tutte le decisioni chiave*** *ed essere considerato internamente come un consigliere fidato che supporta l'azienda in tutti i processi decisionali.*

Oltre al ruolo di abilitatore e suggeritore secondo quanto stabilito per legge, il DPO dovrebbe avere anche un certo numero di **responsabilità operative** in funzione del contesto dell'organizzazione – come, ad esempio,

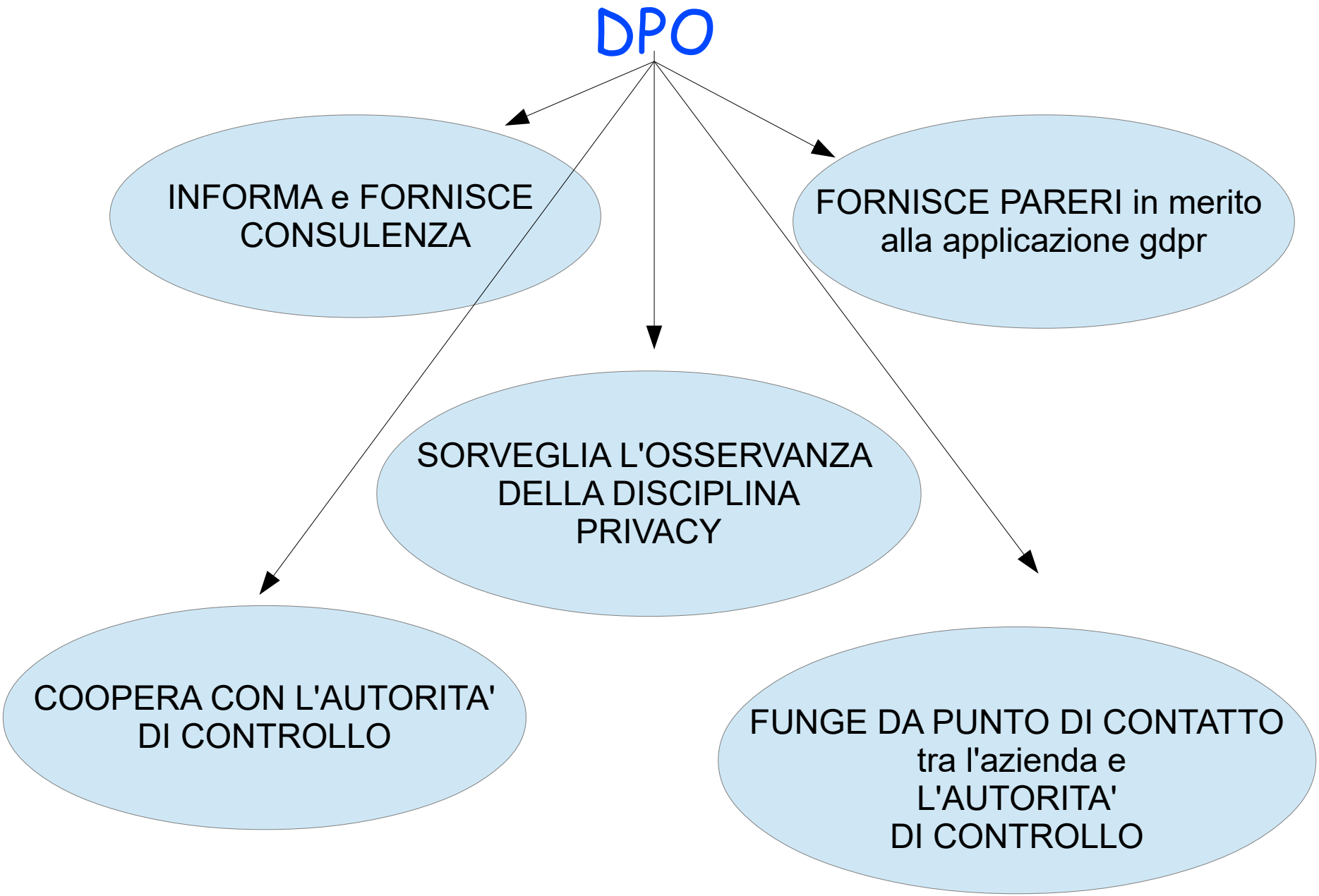
> definizione delle policy,

> gestione delle richieste e dei reclami in materia di dati,

> analisi dei rischi e audit (revisione) della privacy.

Si tratta di un ruolo complesso che richiede, come detto precedentemente, **approfondite conoscenze di questioni legali, di IT, di sicurezza e dei processi di business** in un ambiente in veloce evoluzione. In circa il 50% dei casi il DPO ha un background legale, nel 30% IT, nel 15% di business puro (ad esempio HR) e nel rimanente 5% proviene da ruoli diversi. Le aziende dovranno pertanto assumere e formare gli specialisti.

Il contesto aziendale **determinerà** quali competenze sia meglio cercare in un neoassunto e per quali sia meglio formare la persona (ad esempio, per le aziende molto tecnologiche potrebbe essere necessario assumere un ingegnere esperto con una forte conoscenza dell'IT, una competenza difficile da acquisire senza un background tecnico).


DPO
INFORMA e FORNISCE CONSULENZA
FORNISCE PARERI in merito alla applicazione gdpr
SORVEGLIA L'OSSERVANZA DELLA DISCIPLINA PRIVACY
COOPERA CON L'AUTORITA' DI CONTROLLO
FUNGE DA PUNTO DI CONTATTO tra l'azienda e L'AUTORITA' DI CONTROLLO

L'attenzione va, per prima cosa,

> rivolta all'individuazione **dei massimi rischi** per l'azienda.

Si rende altresì necessaria l'individuazione, all'interno dell'organizzazione, dei RESPONSABILI PRINCIPALI per il GDPR, **in base all'area di riferimento**. Incaricato a svolgere quest'attività è il DPO (data protection officer), ovvero il responsabile della privacy dei dati della società.

Tra i possibili candidati possiamo trovare:

> responsabili HR, per formazione, comunicazioni e dati relativi al personale;

> del settore marketing, per la tutela del brand e dei dati relativi ai clienti;

> infine del reparto IT, per tutto ciò che concerne la sicurezza.

Inoltre dovranno essere esaminate **le cinque aree** di attenzione principali, citate di seguito:

Governance – bisogna stabilire **come tradurre la teoria** del Regolamento **in azioni, norme e valori**. E' necessario anche **valutare quali misure adottare**, la loro efficacia e la possibilità di essere migliorate, secondo la c.d. Privacy by Design.

Comunicazione – è fondamentale, inoltre, **ISTRUIRE** l'organico aziendale sui requisiti della normativa, in particolar modo sui rischi e sull'impatto di un uso improprio dei dati.

Processi – si rende necessario esaminare come il GDPR influenzerà i processi aziendali, quale sarà l'impatto e come potranno esser gestiti i cambiamenti richiesti.

Dati – è basilare offrire la *trasparenza e l'affidabilità* richieste dal GDPR e per poterlo fare è utile regolamentare e garantire la qualità dei dati a disposizione, farne una valutazione, conoscere gli scopi per i quali vengono utilizzati, senza dimenticare di rendere partecipi anche i singoli consumatori, i dipendenti, i clienti o terze parti.

Sicurezza – tutte quelle misure atte alla tutela dei diritti fondamentali della privacy, come la tutela della sicurezza e della riservatezza dei dati personali, ma anche

> l'indicazione di un utilizzo consono,

> gli avvisi,

> il consenso,

> la possibilità di scelta, di accesso, di rettifica o cancellazione.

Questo elemento chiave della normativa può rappresentare un fattore competitivo di differenziazione e porre le basi per una fidelizzazione di clienti e partner commerciali.

Cosa cambia per i dipendenti?

Il nuovo regolamento introduce, come abbiamo visto, tutta una serie di novità che mirano a una **sempre maggiore tutela della privacy**. Per i collaboratori, ciò significa una sempre maggiore garanzia di potersi fidare della propria azienda. Ogni dipendente potrà infatti contare sul fatto che i suoi dati saranno gestiti in maniera corretta e saprà esattamente chi potrà avere accesso a che cosa.

Ai singoli dipendenti viene riconosciuto un maggiore controllo sul modo in cui le imprese possono utilizzare i loro dati.

Le aziende dovranno garantire che i dati siano trattati secondo l'iter stabilito dalla legge, in modo trasparente e al solo scopo per cui sono stati raccolti – per tutti gli altri usi sarà richiesto **esplicito** consenso ai diretti interessati –, ***garantendo la registrazione dei soli dati strettamente necessari al processo di assunzione e di gestione del dipendente e la loro cancellazione quando quest'ultimo non sarà più in azienda.***

In questo modo, dal punto di vista del dipendente, l'introduzione di una tale politica di protezione dei dati più attenta e trasparente potrà concorrere ad aumentare la fiducia dei lavoratori nei confronti della propria azienda e ciò contribuirà, di conseguenza, a creare relazioni sempre più solide e migliori tra le due parti.

GDPR: cambia la disciplina sulla Privacy

Il GDPR **comporta una revisione totale della gestione dei flussi di dati e dei processi aziendali ad essi relativi**, e il risultato di questo cambiamento avrà effetti positivi che riguarderanno sia i singoli individui sia i business aziendali, poiché i primi preferiranno sempre più brand capaci di garantire i loro diritti, mentre le aziende otterranno benefici di ampia portata, tra cui :

> consistenti risparmi di costi, dati da una maggiore efficienza nella gestione dei dati,

> una migliore percezione del brand da parte del mercato.

GDPR: sanzioni pecuniarie molto salate

Il mancato adeguamento alla normativa comporterà sanzioni pecuniarie di notevoli importi, di conseguenza ogni azienda dovrà adottare, entro breve tempo, le misure necessarie per adeguarsi alle novità introdotte. La violazione delle disposizioni del Regolamento può comportare sanzioni pecuniarie fino a 20 Mln € o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. *Possono inoltre aggiungersi eventuali sanzioni civili. E non sono da escludere sanzioni penali*

Perché parlare del GDPR?

alcune novità contenute in esso impongono alle aziende **un'attenta pianificazione**, in quanto comportano modifiche organizzative significative e investimenti di natura tecnologica.

Tra le altre principali novità introdotte dal Regolamento vi sono le seguenti:

a) Principio di «Accountability»

Il GDPR ufficializza il principio di «accountability» (principio di RESPONSABILITA') secondo cui le imprese, titolari dei dati di clienti, dipendenti, consulenti, sono tenute a conformarsi alle normative introdotte nel Regolamento e, in caso di problemi o controlli, comprovare di aver adottato modelli organizzativi, politiche e misure di sicurezza adeguate per la protezione dei dati. Per fare questo **le aziende devono adottare una serie di STRUMENTI indicati nel GDPR.**

>In primis, il **REGISTRO delle ATTIVITA' di TRATTAMENTO** (obbligatorio per aziende con + 250 dipendenti) deve contenere una serie di informazioni, tra le quali :

> nome e i dati di ogni soggetto del trattamento

> le finalità del trattamento,

> le categorie dei soggetti interessati e dei dati personali trattati,

> l'indicazione delle misure di sicurezza adottate.

> le categorie di destinatari a cui i dati personali saranno comunicati

> i trasferimenti di dati personali verso un paese terzo

> i termini ultimi previsti per la cancellazione delle diverse categorie di dati

Questo strumento consente di controllare accuratamente le operazioni di trattamento dati all'interno della società.

Il registro svolge la duplice funzione di :

> strumento operativo, con cui *gestire in maniera ordinata i dati e gli altri elementi utili per assicurare la corretta gestione dei dati personali*,

> di documento tramite il quale il Titolare del trattamento *può dimostrare di aver rispettato la normativa.*

b) Privacy by design/by default

La privacy by design consiste **nell'adozione di misure tecnico-organizzative**, durante la progettazione di un nuovo prodotto o servizio, **a protezione dei dati**, **minimizzando l'uso di questi ultimi per qualsivoglia scopo (privacy by default) e consentendone l'accesso soltanto agli incaricati autorizzati.**

c) Data breach

Obbligo di comunicare all'Autorità competente ed alla clientela, entro 72 ore, eventuali violazioni di sicurezza che comportano in modo accidentale o illecito la distruzione, la perdita, la modifica, la diffusione o l'accesso, non autorizzati, ai dati personali.

d) Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati)

È necessario valutare **preventivamente l'impatto privacy per limitare la possibilità e gravità dei rischi per i diritti e le libertà dei soggetti terzi in base alla loro natura, portata o finalità.** Questo processo consente di acquisire le competenze necessarie riguardo le misure, le garanzie e i meccanismi previsti per ridurre i rischi e assicurare la conformità del trattamento alla normativa.

e) Data Protection Officer (artt. 37-39)

Obbligo per imprese ed enti, che trattano o controllano dati sensibili su larga scala, di incaricare un Data Protection Officer per la verifica dell'applicazione del Regolamento.

Pseudonimizzazione

Strumento fondamentale per l'ottenimento della protezione dei dati su larga scala, nel caso in cui *non si possa evitare del tutto l'uso di dati personali*. Si tratta di un processo volto a «**mascherare** l'identità» di una persona, **non a celarla**. La pseudonimizzazione rappresenta una **misura di sicurezza** in quanto consente di **ridurre la correlabilità** di un insieme di dati ad un determinato soggetto.

Misure di sicurezza

Il Regolamento prevede l'adozione di misure idonee a garantire un livello di sicurezza adeguato al rischio dei trattamenti e alla natura dei dati. Gli adempimenti richiesti alle imprese si dividono nelle seguenti due categorie:

1. **valutazione dei rischi relativi al trattamento dati;**
2. **attuazione di misure per limitare i rischi.**

Le aziende devono mettere in atto misure di sicurezza che bilancino da una parte l'evoluzione tecnologica e dall'altra i rischi per i diritti e le libertà delle persone che i trattamenti comportano.

RIASSUMENTO : principi cardine

I principi cardine della GDPR riguardano: **trasparenza, finalità, minimizzazione, conservazione e le misure tecniche ed organizzative adeguate.**

E' bene ricordare che dare visibilità agli interessati dei dati raccolti e delle finalità del trattamento, è una regola già presente nei principi del Codice Privacy; essa viene solamente rafforzata in ambito europeo.

Per rispondere in modo efficace alle misure di sicurezza richieste, dove possibile, i dati vanno **razionalizzati**. Questo processo, che tenga conto dei citati cardini del Regolamento, è occasione di riorganizzazione e ottimizzazione interna.

Razionalizzazione che, come accennato, dovrà coinvolgere anche i rapporti con tutti i soggetti esterni che, a vario titolo, sono coinvolti in attività aziendali che abbiano ricadute sul trattamento dei dati.

IL GDPR obbliga le aziende a presentarsi preparate, nel loro complesso, ad accettare e promuovere una prospettiva di tutela del patrimonio informativo che abbraccerà, in modo integrato, la totalità delle attività di business per esser efficace.

FINE

ANDRIOLI & PARTNERS
Centro Studi
Giuridici Finanziari Aziendali

Alessandra Andrioli

342.6809202

studioandrioli@gmail.com -
www.andriolimayersonconsulenzadirezionale.com

bologna@profiliecarriere.it - www.profiliecarriere.it