mailup
BE RELEVANT

GDPR & dati personali

Novità, cambiamenti e attività da intraprendere

IL CONTO ALLA ROVESCIA È SCATTATO: COME **METTERE A NORMA** LA TUA AZIENDA IN BASE AL **NUOVO REGOLAMENTO EUROPEO** SUI DATI PERSONALI

WHITEPAPER
Passione per l'email marketing

Hanno collaborato a questo white paper

Avv. Marco Maglio

Presidente dell'Osservatorio Europeo sulla Data Protection
Avvocato, fondatore di Lucerna Iuris, Network Giuridico Internazionale formato da studi legali specializzati in diritto del marketing e della comunicazione. Presiede il Giurì per l'Autodisciplina del direct marketing e del commercio elettronico e l'Osservatorio Italiano Privacy. Partecipa alle attività dei principali Gruppi di lavoro formati da Esperti Internazionali in materia di Data Protection e Marketing Law. È Componente del Legal Affairs & Ethics Committee di FEDMA (Federazione Europea del Direct Marketing) in rappresentanza dell'Italia, membro dell'International Privacy Professionals Association e Senior Certified Privacy Auditor.

MARIA GIULIA GANASSINI

Content & Community Manager @MailUp
Classe 1984, milanese atipica, la sua formazione mescola Lettere Classiche e Digital Marketing. Lavora nell'editoria a Milano e a Londra, si occupa di eventi culturali nei Balcani, e per tre anni dirige la comunicazione della startup LOVEThESIGN. Dal 2016 è Content Manager per MailUp: l'obiettivo è svelare il mondo complesso e articolato che si cela dietro il bottone "invia" di ogni email. Nel resto del tempo legge, viaggia e studia lingue straniere.

Indice

Prefazione

DI **MARCO MAGLIO**

La tutela dei dati personali, fino a poco più di vent'anni fa, non conosceva in Italia nessuna regolamentazione. Era il **1996** quando per la prima volta il legislatore italiano si è occupato di **proteggere** ognuno di noi dall'**utilizzo improprio delle informazioni individuali**. Il mondo era molto diverso da quello che è oggi e anche i dati riferiti alle persone erano limitati e di difficile reperimento. Erano essenzialmente informazioni identificative, dati oggettivi, di recapito ed erano contenuti in elenchi o archivi. Erano soprattutto **dati statici**, non modificabili e le possibilità di abuso erano limitate. Eppure già vent'anni fa si sentì la necessità di una disciplina rigorosa che permettesse di garantire il diritto di ogni persona di **esercitare un controllo** sulle informazioni che la riguardano. Peraltro in quell'epoca una prima direttiva comunitaria imponeva a tutti gli stati europei di dotarsi di regole comuni per permettere la libera circolazione delle informazioni nel territorio del mercato economico europeo.

Dal 1996 è iniziato un **diluvio di norme** volte a regolamentare l'attività di comunicazione, l'uso di strumenti che si basano sulla **tecnologia informatica** e **l'utilizzo di database**. Queste regole si intrecciano sempre più strettamente con questioni che vanno oltre gli aspetti di carattere strettamente giuridico. Nel corso degli ultimi venti anni tanto il legislatore dell'Unione Europea quanto quello nazionale hanno emanato norme, leggi e regolamenti che incidono profondamente sull'acquisizione e sull'uso di informazioni riferite o riferibili agli individui.

E ognuno di noi ha acquisito con crescente sicurezza una piena consapevolezza dei propri diritti circa l'uso che altri possono fare delle informazioni che ci riguardano: per questo motivo il mancato rispetto della normativa diventa fonte di **grave rischio sanzionatorio**.

Le nuove tecnologie rendono sempre più facile **raccogliere dati ed elaborarli** confrontandoli con gli enormi database che si generano mentre noi usiamo gli oggetti collegati alla rete. L'**Internet delle cose, i big data, il behavioural advertising**, gli **strumenti predittivi** sono al tempo stesso fonti di dati personali e depositi enormi di conoscenza generata mettendo insieme informazioni riferite a individui.

Anche per questo motivo è diventato essenziale prevenire possibili violazioni legali e acquisire una conoscenza di base in grado di indicare come muoversi in questo ambito, che oggi è fortemente regolamentato.

Proprio per effetto di questa evoluzione l'**Unione Europea** ha deciso di emanare un **Regolamento Generale sulla tutela dei dati personali**, che dal **2018** definisce regole uniche per tutti i trattamenti di dati effettuati nel territorio dei Paesi Membri dell'Unione.

Diventa quindi essenziale, e non solo per chi si occupa di questioni giuridiche, conoscere i principi che regolano l'uso dei dati personali: in questo modo sarà possibile individuare tempestivamente le questioni che possono derivare da una determinata attività e operare con sufficiente tranquillità, **riducendo i rischi legali**.

Con questa chiave di lettura è possibile dedicare alla data protection particolare attenzione, mettendo in evidenza i principi generali e le questioni applicative essenziali.

Buona lettura!

Avv. Marco Maglio

*In questi vent'anni i dati personali sono diventati sempre più importanti e la loro natura è cambiata. Non sono più solo un bene che è importante proteggere per prevenire violazioni dei diritti fondamentali delle persone cui si riferiscono. Sono diventati un bene economico, sono anzi la materia prima essenziale dell'**Economia della Conoscenza e dell'Informazione**. E senza dati personali la stessa idea di Sharing Economy sarebbe inimmaginabile.*

Introduzione

CHE COS'È IL GDPR?

*Il GDPR come **Statuto della Data Economy**: il dato come moneta dell'economia dell'informazione.*

GDPR è l'acronimo di **General Data Protection Regulation**. È la sigla che ormai abitualmente designa il Regolamento (UE) 2016/679 emanato il **27 aprile 2016** che stabilisce le regole valide in **tutti i paesi dell'Unione Europea** in materia di dati personali senza necessità di leggi nazionali di recepimento.

Il GDPR marca una linea di confine nell'evoluzione storica della data protection. È uno spartiacque che segna un "prima" e un "dopo", l'inizio di una nuova epoca nelle norme che **tutelano il diritto a esercitare un controllo sulle informazioni** che riguardano una persona fisica.

Il cambiamento essenziale è costituito dal cambio di prospettiva che si realizza grazie alle nuove norme. Finora al centro delle normative di data protection è stata posta la persona, intesa come **persona fisica**, titolare di diritti, depositario di interessi legittimi e di aspettative che l'ordinamento riconosce e tutela.

Conseguentemente a questa impostazione l'interessato, cioè il soggetto cui si riferiscono i dati personali, è sempre stato considerato il vero protagonista della normativa. Questo è il motivo per cui vengono introdotti con la normativa degli anni Novanta i principi del **consenso informato**, del **diretto potere di controllo** degli interessati, del **diritto a opporsi al trattamento dei dati**. Si proteggono i dati per proteggere la persona cui i dati si riferiscono.

Con l'evoluzione tecnologica tutto cambia. **I dati acquistano valore in sé** e vengono tutelati per ciò che sono, a prescindere, si potrebbe dire, dalle persone cui si riferiscono.

Il dato personale diventa **la materia prima** della nuova economia basata sulla conoscenza e sull'elaborazione delle informazioni. I dati infatti vengono ormai considerati un potenziale **motore per lo sviluppo** e una **fonte di nuovi business**

ad altissimo valore.

È questo il motivo per cui **la Commissione Europea** ha dato estrema importanza alla tematica della protezione dei dati personali inserendola nel più ampio contesto dei cosiddetti **open data**.

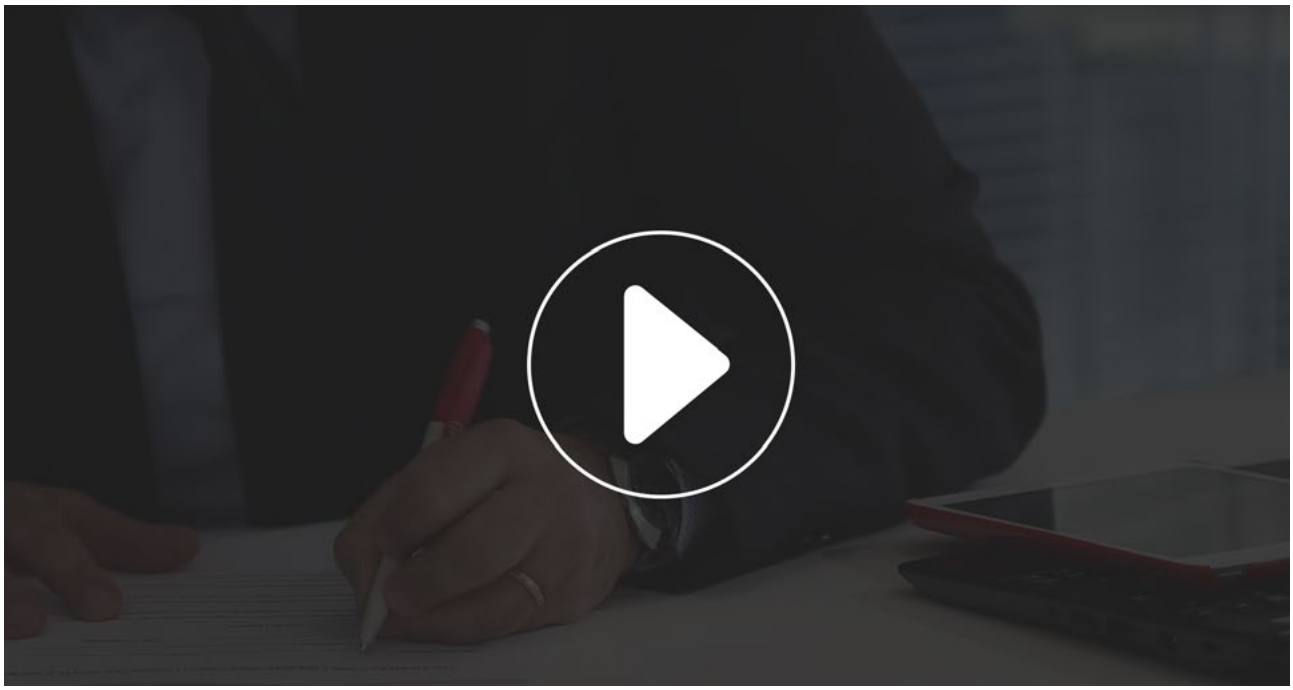
In pratica si è compreso che i dati sono destinati a diventare sempre di più la materia prima che sarà alla base dei servizi e dei prodotti innovativi e solo creando le condizioni per un **uso uniforme dei dati**, senza barriere giuridiche e differenze normative tra gli Stati europei, si potrà definire una **nuova economia basata sull'uso esteso dei dati**. In questo senso il regolamento Europeo 2016/679 diventa uno strumento di competizione economica rilevante che permette ai soggetti operanti nel Mercato Europeo di disporre di un **set di regole condivise** cui anche chi è posto fuori dall'Unione Europea sarà obbligato ad attenersi. Si tratta di una regola nuova che trasforma la protezione dei dati personali da mero argomento giuridico in **tema strategico** per la nuova economia dei dati.

Il GDPR nasce per essere quindi lo **Statuto della Data Economy** e definisce le regole per usare i dati legalmente ed estrarne prodotti e servizi, quindi fatturato e posti di lavoro.

In ciascun capitolo del white paper, l'Avv. Marco Maglio approfondisce un aspetto legato al GDPR. **Il video e il testo sono complementari**: per assicurarti di non perdere nessuna informazione importante, seguili entrambi! Se non visualizzi correttamente i video, clicca sul link abbinato per guardarli su YouTube.

Che cosa comporta il GDPR per le aziende?

CAPITOLO 1



Se non visualizzi correttamente il video, guardalo qui

Tutti trattano **dati personali**, siano quelli dei clienti, dei prospect, dei dipendenti o dei fornitori; l'argomento attraversa sostanzialmente ogni attività umana. Finora siamo stati abituati a considerare la **privacy come un adempimento**, un **obbligo** da rispettare con comportamenti formali, affidati di solito alla supervisione di un legale.

Con il regolamento europeo cambia tutto: la privacy diventa un **processo aziendale** da gestire in tutte le sue fasi, da quella ideativa a quella esecutiva. Il concetto alla base del cambiamento è semplice: i dati personali sono diventati l'equivalente della **materia prima** per l'economia tradizionale, l'elemento base da trasformare nel prodotto per il mercato. I dati sono **il "petrolio" dell'era digitale**, l'elemento che va elaborato per generare i fatturati delle aziende. In estrema sintesi, oggi i dati personali servono a:

1. Creare prodotti innovativi
2. Formulare offerte mirate ai consumatori, convertendo sconosciuti in clienti fidelizzati
3. Garantire sicurezza e migliorare l'efficienza aziendale
4. Controllare, profilare e analizzare

Alla luce dell'importanza che i dati hanno

assunto nell'economia attuale diventa essenziale proteggere il processo produttivo che si genera attorno ai dati e **prevenire possibili abusi nell'utilizzo delle informazioni riferite agli individui**.

Ma cosa cambia oltre all'approccio? In due parole, cambia tutto:

1. Cambia l'informativa che diventa **breve**, priva di riferimenti normativi, deve essere **comprensibile anche ai minori e** contenere nuovi elementi, come l'**origine dei dati** e il **tempo di conservazione previsto**.
2. Cambia il consenso al trattamento che cessa di essere necessariamente espresso e diventa un **consenso inequivocabile** e quindi **desumibile in base ai comportamenti** degli interessati.
3. Cambiano i ruoli del trattamento, con l'introduzione della figura del **Data Privacy Officer** (il responsabile per la protezione dei dati personali) che sarà un vero manager dei database aziendali e non un semplice garante interno del legittimo trattamento dei dati.
4. Sparisce l'obbligo di notificazione al Garante e si introduce il **registro dei trattamenti**
5. Sparisce il Documento programmatico sulla sicurezza e nasce il **Documento di valutazione di impatto** del trattamento dei dati.
6. Vengono introdotti **meccanismi di certificazione** e nascono i cosiddetti **Sigilli di qualità della Privacy**.
7. Vengono introdotti **nuovi diritti**, come quello alla **portabilità dei dati**, per cui ogni interessato potrà trasferire da un titolare a un altro i dati che lo riguardano.
8. Diventa essenziale **progettare la tutela dei dati personali** e **documentare l'attenzione verso l'analisi dei rischi** connessi al trattamento dei dati personali.
9. Le norme **seguono il soggetto cui si riferiscono i dati**: ogni cittadino europeo ha diritto di vedere applicato il regolamento europeo anche quando i dati sono raccolti da una società extraeuropea.
10. **Le sanzioni in caso di violazione aumentano** significativamente e per le multinazionali sono calcolate in percentuale (fino al 4%) del fatturato del Gruppo.

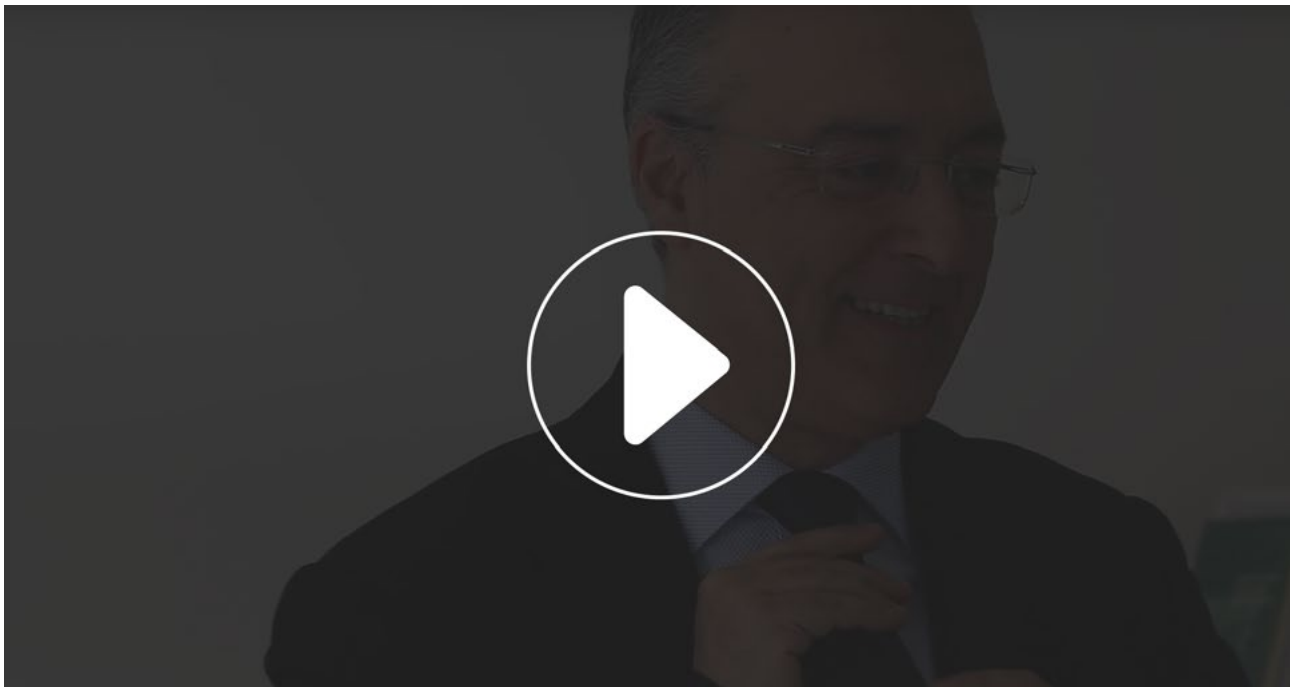
> I dati sono il petrolio dell'era digitale, l'elemento che va elaborato per generare i fatturati delle aziende.

L'obiettivo di queste regole è **porre fine alle numerose restrizioni** di carattere giuridico o amministrativo che, sotto forma di obblighi, impongono la gestione locale dei dati a livello nazionale che vincolano l'intero mercato UE dei dati. L'abolizione di queste restrizioni potrebbe generare **8 miliardi di euro all'anno di Prodotto Interno Lordo**.

Per cogliere da subito le tante **opportunità** che si aprono per le aziende grazie alla nuova era della privacy occorre **agire subito**, mappare le proprie banche dati, ripensare i processi di trattamento dei dati e impegnarsi per estrarre valore dalle informazioni di cui si dispone nel rispetto degli interessati. Solo così si potrà raggiungere l'obiettivo vero di questa riforma: permettere alle imprese di dire "**Privacy is good for business**".

Un nuovo modello organizzativo

CAPITOLO 2



Se non visualizzi correttamente il video, guardalo qui

Con le nuove regole cambia profondamente l'approccio alla tutela dei dati, che cessa di essere un insieme di adempimenti e diventa un processo produttivo, da gestire mediante un **modello organizzativo specifico**.

Con il nuovo Regolamento UE 679/2016 in materia di dati personali si assiste a un cambiamento di prospettiva della disciplina di riferimento. In particolare, mentre la vecchia normativa si basava sui diritti dell'interessato, il nuovo quadro normativo è incentrato sui **doveri** e sulla **responsabilizzazione** (accountability) del titolare del trattamento.

Se il Codice in materia di dati personali (D.Lgs. 196/2003) aveva indicato ai titolari del trattamento un elenco di misure minime di sicurezza da adottare, senza le quali erano previste sanzioni, la nuova normativa sposta la scelta e la responsabilità su

quali misure **tecniche e organizzative** sia opportuno adottare sul titolare del trattamento.

Ai titolari del trattamento nel settore pubblico e privato è richiesto non semplicemente di rispettare le norme, e quindi di fare una check-list degli adempimenti minimi, ma di **tradurre in pratica questi princìpi** con diverse azioni concrete. Dovranno dimostrare di aver distribuito responsabilità al proprio interno, di avere una risposta per i vari problemi, di aver valutato i rischi e le possibili conseguenze, e quindi di avere una **strategia articolata e trasparente** nei confronti dei soggetti cui si riferiscono le informazioni.

Da insieme di adempimenti a processo produttivo: ***la data protection come strategia aziendale****, articolata e trasparente.*

La Data Protection non è più una materia delegabile a un consulente, a un esperto di tecnologia o a un ufficio legale. Sarà proprio l'**approccio organizzativo dell'imprenditore** che avrà importanza, anche perché si dovranno individuare linee di bilancio importanti.

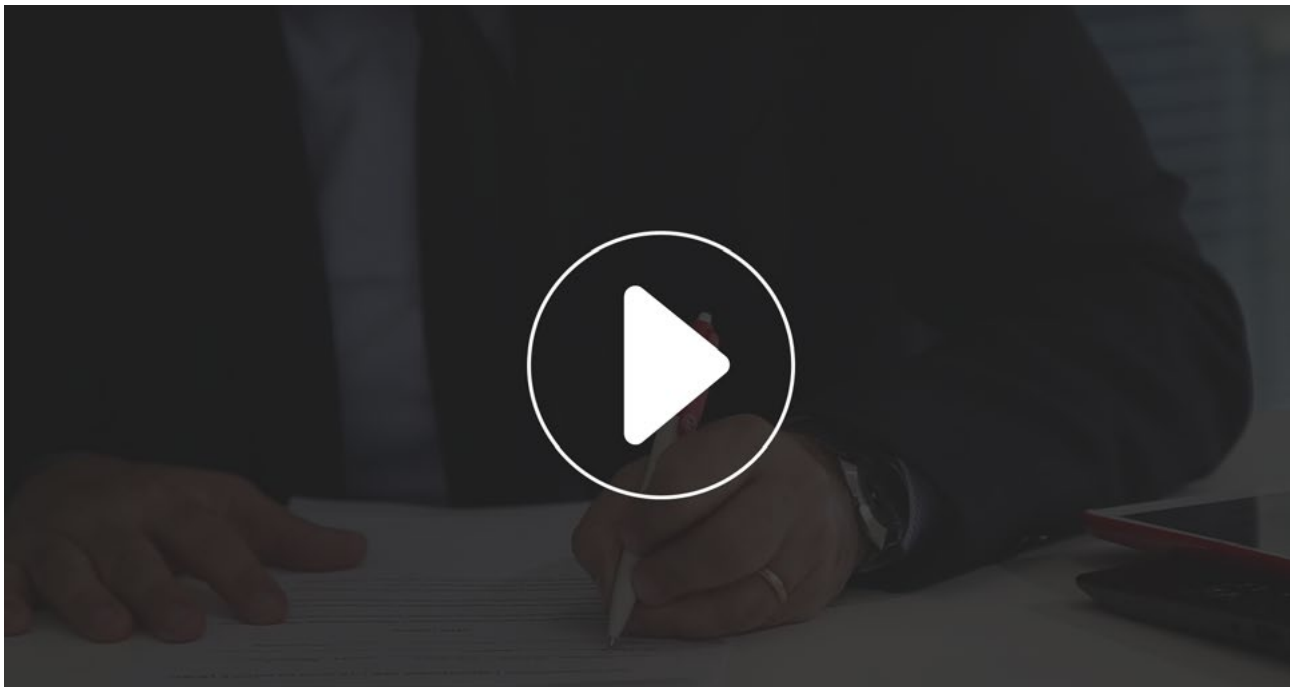
Con il nuovo regolamento, il titolare quindi ha un ruolo più **proattivo** e soprattutto **obblighi più pregnanti**, finalizzati non soltanto al formale rispetto delle regole, ma anche all'adozione di tutti gli accorgimenti tecnici e organizzativi necessari a **garantire la compliance** effettiva dei trattamenti, anche sotto il profilo della sicurezza.

Ma come si deve comportare quindi il titolare del trattamento per essere conforme al principio di accountability? Come farà a dimostrare di aver adottato senza convenzionalismi tutte le misure privacy richieste dal Regolamento?

La soluzione prospettata dalle nuove normative prevede che sia onere di chi tratta dati predisporre dei **processi di valutazione di impatto** del trattamento dei dati personali e che si realizzino quindi dei **risk assessment** connessi alla data protection. Si accentua la necessità di maggiore garanzia dell'effettiva protezione.

Come cambia l'informativa

CAPITOLO 3



Se non visualizzi correttamente il video, guardalo qui

L'informativa cambia e diventa finalmente uno **strumento di informazione**, cessando di essere un adempimento.

Il titolare deve fornire all'interessato tutte le informazioni relative al trattamento in **forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro**, in particolare nel caso di informazioni destinate specificamente ai minori.

Oltre che per iscritto o con mezzi elettronici, le informazioni possono essere fornite anche **oralmente**, ma solo se lo chiede l'interessato e se la sua identità è comprovata.

Le informazioni possono essere **rese abbinando il testo a icone standardizzate per dare** un quadro d'insieme del trattamento previsto.

Nulla impedisce di fornire informazioni in modo graduale. Si parla di **informativa a strati**, che rende l'informazione in modo sintetico, rimandando specifiche e appro-

fondimenti a link o pop up. Ecco allora una **check list** per verificare la completezza della tua informativa.

VERIFICA SE LA TUA INFORMATIVA CONTIENE QUESTI ELEMENTI	SÌ	NO
a) L'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante		
b) I dati di contatto del responsabile della protezione dei dati, ove applicabile		
c) Le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento		
d) Se il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, i legittimi interessi perseguiti dal titolare del trattamento o da terzi		
e) Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali		
f) Ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione		
g) Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo		
h) L'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati		
i) L'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca		
l) Il diritto di proporre reclamo a un'autorità di controllo		
m) Se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati		
n) L'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.		

Come raccogliere il consenso al trattamento

CAPITOLO 4

Se non visualizzi correttamente il video, guardalo qui

Siamo abituati a considerare il consenso valido solo se formulato con una **dichiarazione espressa** (è l'effetto del cosiddetto sistema dell'opt in, che l'Italia ha adottato con convinzione fin dal 1997, anno di entrata in vigore della prima normativa sui dati personali).
Oggi si introduce un approccio di chiaro sapore anglosassone, meno formalista e **più sostanziale**.
Secondo il nuovo regolamento europeo (così recita il Considerando 25 del testo approvato), *"il consenso dovrebbe essere espresso mediante un'**azione positiva inequivocabile** con la quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di **accettare che i dati personali** che lo riguardano **siano oggetto di trattamento**, ad esempio mediante dichiarazione scritta, anche elettronica, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni*

tecniche o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in questo contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso ***il consenso tacito o passivo o la preselezione di caselle****. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere dato per l'insieme delle finalità del trattamento. Se il consenso dell'interessato è richiesto con modalità elettronica,* ***la richiesta deve essere chiara, concisa e non disturbare*** *inutilmente il servizio per il quale il consenso è espresso".*

Il consenso dell'interessato come manifestazione di volontà espressa mediante dichiarazione o azione positiva inequivocabile.

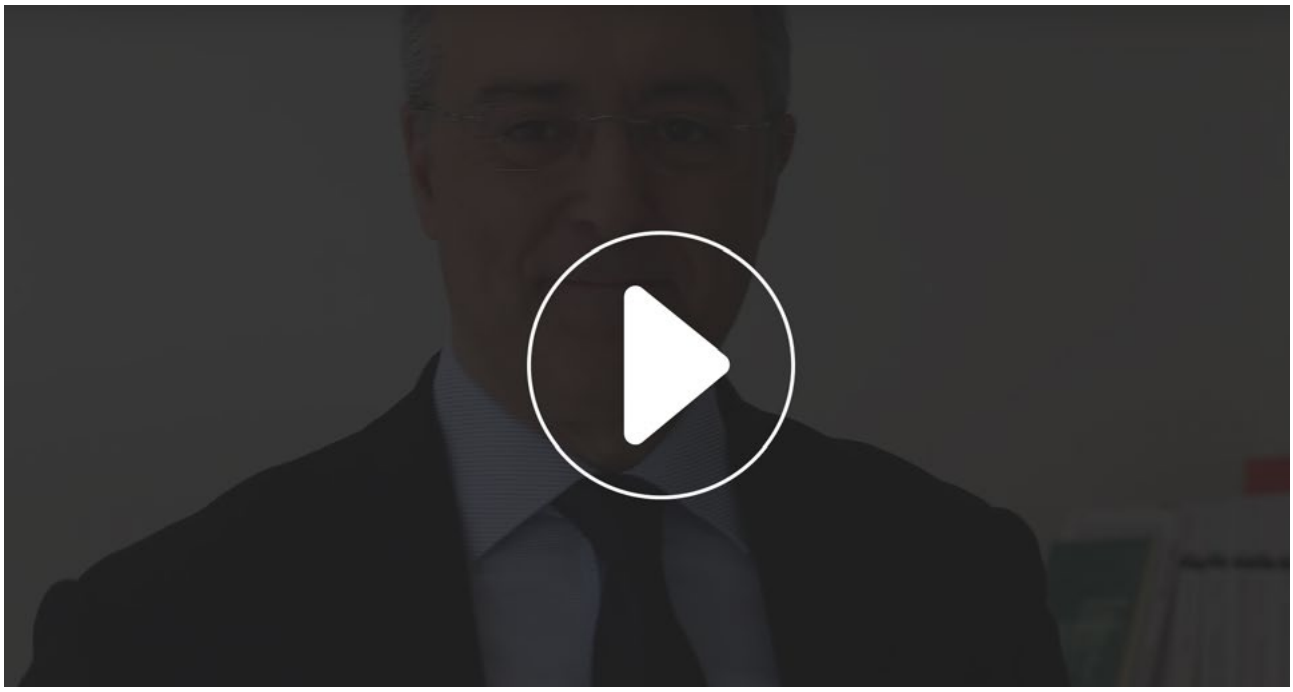
Questo di fatto dà spazio, entro certi limiti, a forme di consenso desunto da comportamenti concludenti espressi mediante **azioni positive** da parte dell'interessato. È un importante cambiamento che apre spazi nuovi rispetto ai rigidi steccati dell'opt in, che pure restano formalmente in piedi. Va tenuto conto che la definizione di **"consenso dell'interessato"** fornita dal regolamento è questa: "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile con la quale l'interessato accetta, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento."

È quindi sparito il riferimento, originariamente previsto dal testo, al carattere esplicito del consenso che, a certe condizioni, si può desumere in base al **comportamento attivo** dell'interessato.

Un esempio tipico di **consenso non equivoco**, manifestato con azioni positive, è quello reso quando, visualizzando un banner che ci informa che il sito che stiamo visitando utilizza **cookies**, continuiamo a navigare - di fatto accettando l'uso dei cookies.

L'analisi del rischio: cos'è e come si crea

CAPITOLO 5



Se non visualizzi correttamente il video, guardalo qui

Per anni siamo stati abituati a gestire un adempimento formale denominato **Documento Programmatico sulla Sicurezza (DPS)**, una fotografia documentata dell'adeguatezza delle misure di sicurezza adottate per trattare i dati personali.

Nel 2012 tale adempimento ha cessato di essere obbligatorio, ma con il nuovo regolamento europeo dovremo presto imparare a destreggiarci con nuovo strumento: il **Data Protection Impact Assessment (DPIA)**, ovvero il documento di valutazione di impatto nel trattamento dei dati.

Sarà una vera e propria analisi dei rischi in concreto generati dal trattamento dei dati aziendali. Chi raccoglie i dati dovrà effettuare una **valutazione degli impatti** determinati dal trattamento dei dati stessi fin dal momento della progettazione del processo aziendale e degli applicativi informatici di supporto, in particolare nei casi in cui il trat-

tamento presenti **rischi specifici per i diritti e le libertà degli interessati**.

Il processo prevede **tre distinte fasi** da svolgersi periodicamente con cadenza almeno annuale:

1. Analisi dei rischi
2. Definizione della lista delle criticità (gap list)
3. Definizione del programma di intervento (action plan)

La probabilità e la gravità del rischio legato al trattamento dei dati dovranno essere determinate in funzione della natura, del campo di applicazione, del contesto e delle finalità del trattamento dei dati. Sarà **una vera e propria rivoluzione** per quanti sono abituati alle cadenze confortevoli del DPS e all'approccio tecnico informatico alla materia.

*Più che un adempimento, **un'auto-verifica preliminare** con cui le aziende valutano i rischi implicati dal trattamento.*

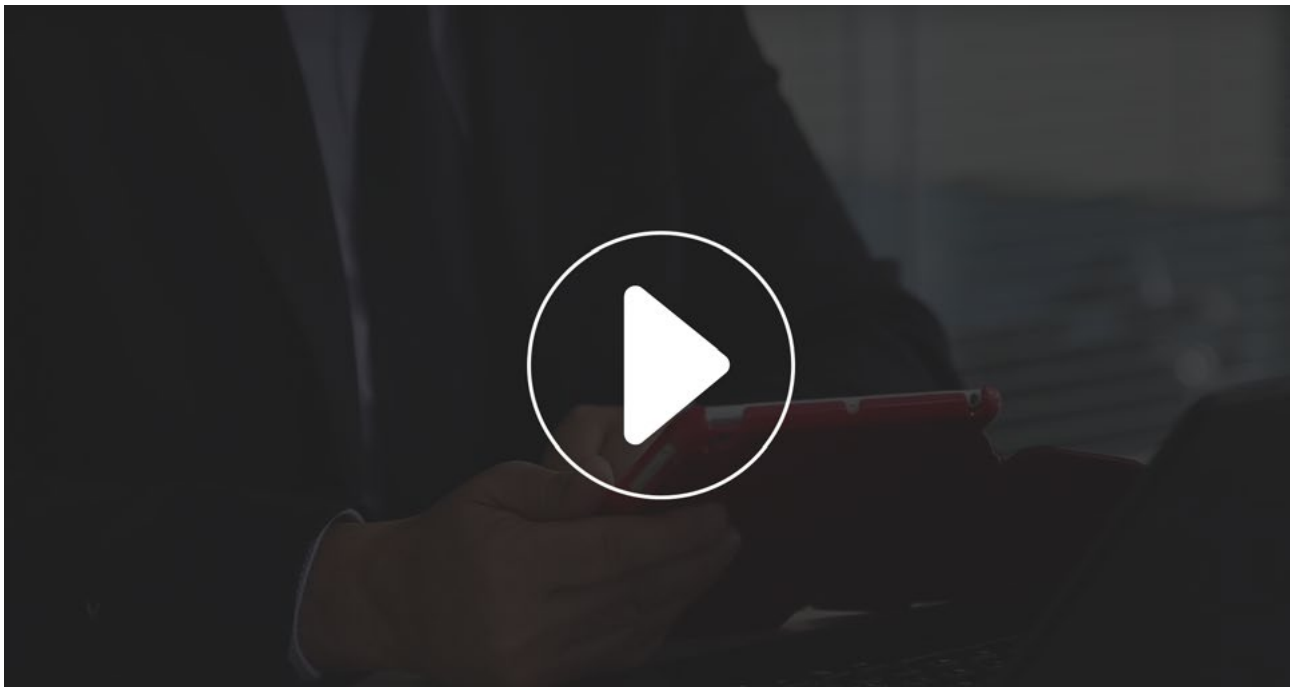
Con il DPIA viene introdotta un'analisi dei processi aziendali profonda che mira a **gestire i rischi, prevedendoli**.

In un'ottica di responsabilizzazione dei titolari del trattamento, il DPIA potrebbe essere infatti visto come una "**auto-verifica preliminare**" che ciascun titolare svolge autonomamente per avere contezza di quali sono i rischi che il trattamento dei dati comporta.

Solo quando, in base ai risultati del DPIA, si rilevi un **alto rischio** per le attività di trattamento dati, il titolare può chiedere all'autorità Garante di pronunciarsi in merito al trattamento in questione, richiedendo una **consultazione preventiva**.

Come cambiano i rapporti con il Garante

CAPITOLO 6



Se non visualizzi correttamente il video, guardalo qui

Fino a oggi, chi effettuava alcune tipologie di **trattamenti** (ad esempio geolocalizzazione, ricerca genetica, profilazione, analisi sulla puntualità dei pagamenti e altre tipologie di trattamenti particolarmente invasivi) era tenuto a effettuare un **adempimento preventivo**: la notificazione al Garante per la protezione dei dati personali.

Con la riforma europea dal 2018 cambia tutto. Viene **abolito l'obbligo di Notificazione** di specifici trattamenti all'Autorità Garante.

Tale adempimento è considerato dal Legislatore europeo come un obbligo che comporta **oneri amministrativi e finanziari**, senza aver mai veramente contribuito a migliorare la protezione dei dati personali (in particolare per le piccole e medie imprese).

Si è quindi deciso di abolire tale obbligo

generale di notificazione, sostituendolo con meccanismi e procedure efficaci che si concentrino piuttosto su quelle operazioni di trattamento che, potenzialmente, presentano **rischi specifici** per i diritti e le libertà degli interessati, per la loro natura, portata o finalità.

L'obbligo di notificazione non scompare del tutto, ma viene sostituito da un nuovo documento: il **registro del trattamento**. Il GDPR prevede che, su richiesta, il titolare o il responsabile del trattamento mettano a disposizione dell'autorità di controllo il registro dei trattamenti. Spetta al **titolare** l'obbligo di documentazione della conformità della propria organizzazione alle prescrizioni della legge. Obbligo che grava anche sul **responsabile**, per i trattamenti che questi svolga per conto di un titolare.

L'obbligo di redazione e adozione del registro non è, tuttavia, generale. Esso non compete "alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati, o i dati personali relativi a condanne penali e a reati".

Nella redazione del registro occorre rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di **informazione**, **consapevolezza** e **condivisione** interna. Bisogna inoltre costituire lo strumento di **pianificazione** e **controllo** della politica della sicurezza di dati e banche di dati, tesa a garantire la loro integrità, riservatezza e disponibilità.

Il registro deve contenere:

- **Il nome e i dati di contatto** del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati.
- **Le finalità** del trattamento.
- **Una descrizione delle categorie** di interessati e delle categorie di dati personali.
- **Le categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali.
- Ove applicabile, **i trasferimenti di dati personali** verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, e la documentazione delle garanzie adeguate.
- Ove possibile, **i termini ultimi** previsti per la cancellazione delle diverse categorie di dati.
- Ove possibile, **una descrizione generale** delle misure di sicurezza tecniche e organizzative.

Il registro del trattamento deve documentare la conformità delle attività di trattamento alle prescrizioni di legge.

Il Data Privacy Officer

CAPITOLO 7

Se non visualizzi correttamente il video, guardalo qui

Se fino a oggi eravamo abituati a prevedere i **tre ruoli classici** nel trattamento dei dati (titolare, responsabile ed incaricato), prepariamoci a un grosso cambiamento. A parte le novità puramente terminologiche (noi italiani scopriremo infatti con sorpresa che quello che chiamiamo Titolare nel linguaggio europeo si chiama Responsabile del trattamento, ed è colui che definisce le finalità del trattamento; chi noi chiamiamo oggi Responsabile nella terminologia europea viene chiamato Incaricato; quelli che noi chiamiamo incaricati non sono previsti dal nuovo ordinamento europeo), prepariamoci a veder nascere una nuova stella nel firmamento della privacy aziendale. Nel 2018 nascerà infatti la figura del **Data Privacy Officer** (DPO) o meglio del **Responsabile della protezione dei dati personali**.

Sarà una figura obbligatoria se:
a) Chi tratta i dati è un soggetto pubblico

b) Si trattano rilevanti quantità di dati personali
c) Si trattano sistematicamente dati sensibili o giudiziari

Il DPO, che può essere un consulente esterno all'azienda, deve possedere requisiti di **professionalità**, **indipendenza** e **autonomia di spesa**, diventando una sorta di auditor interno dei processi di trattamento dei dati personali e il referente che il Garante contatterà in caso debba acquisire informazioni o formulare contestazioni rivolte a chi tratta i dati personali in azienda.

Figura indipendente e con autonomia di spesa, *il Data Privacy Officer gestisce i rapporti con l'Autorità e i vari soggetti aziendali preposti al trattamento*

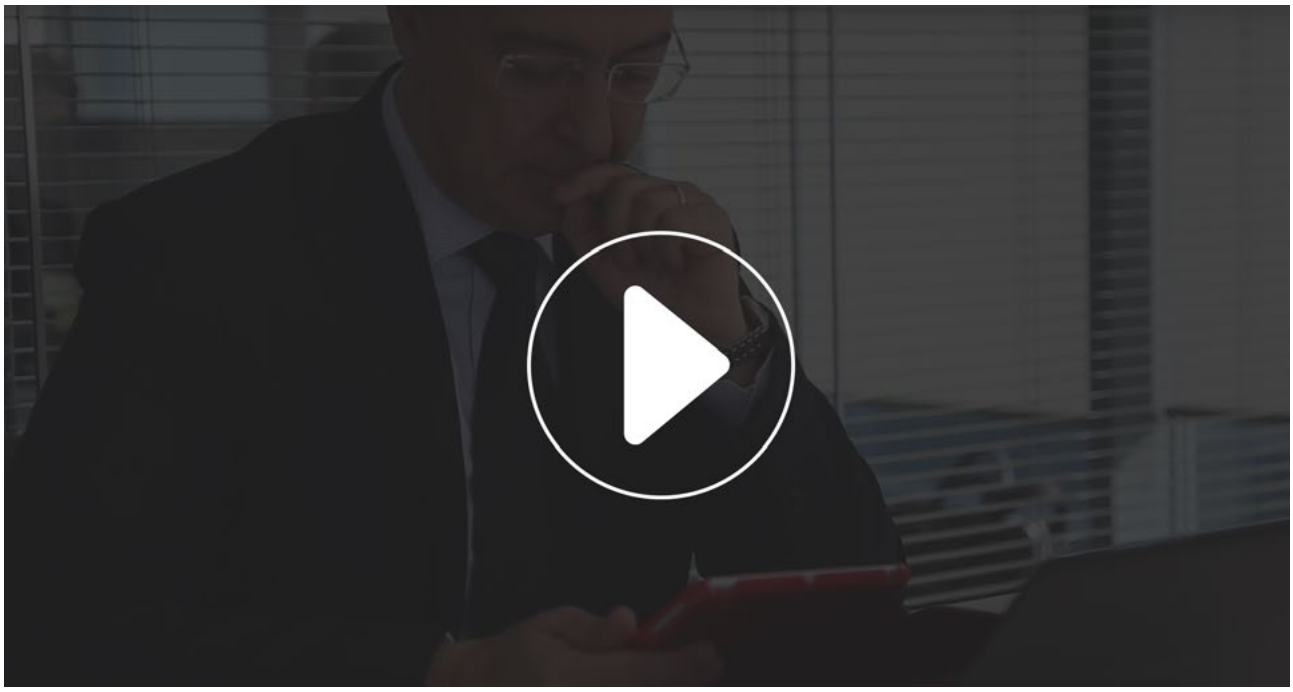
I compiti essenziali del DPO sono i seguenti:

- **Informare e consigliare** il titolare o il responsabile del trattamento in merito agli obblighi derivanti dal regolamento europeo e conservare la documentazione relativa a tale attività e alle risposte ricevute.
- **Vigilare sull'attuazione** e sull'applicazione delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi.
- **Verificare l'attuazione** e l'applicazione del Regolamento europeo; la sicurezza dei dati; il riscontro alle richieste degli interessati di esercitare i diritti riconosciuti dal Regolamento.
- **Garantire la conservazione** della documentazione relativa ai trattamenti effettuati dal titolare.
- **Controllare** che le violazioni dei dati personali siano documentate, notificate e comunicate.
- **Controllare** che il titolare o il responsabile del trattamento effettui la valutazione d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva nei casi previsti.
- **Fungere da punto di contatto** per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.
- **Controllare** che sia dato seguito alle richieste del Garante per la protezione dei dati personali e, nell'ambito delle sue competenze, cooperare di propria iniziativa o su richiesta dell'Autorità.

La scelta del DPO va fatta tenendo conto della natura dei trattamenti effettuati e delle complessità da gestire. È importante che la persona scelta per gestire questo ruolo abbia **esperienza**, **competenza** e sia in grado di gestire i **rapporti con l'Autorità**, con i vari responsabili e con gli altri soggetti preposti al trattamento

Privacy by design e Privacy by default

CAPITOLO 8



Se non visualizzi correttamente il video, guardalo qui

Il senso del GDPR si potrebbe sintetizzare in una frase: "Tratta meno dati che puoi e, se devi trattarli, fallo organizzandoti in modo da prevenire i rischi".

Questo criterio di comportamento è espressione del **principio di minimizzazione** dell'uso dei dati che prevede che i dati trattati devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il **perseguimento delle finalità** per cui sono raccolti e trattati.

Questo significa che il Titolare del trattamento richiede l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla **limitazione** della finalità, alla **minimizzazione** dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie

particolari di dati personali, le misure a garanzia della sicurezza dei dati.
Vengono introdotti nel sistema normativo europeo **due nuovi principi fondativi** dall'approccio evoluto al corretto trattamento dei dati personali: la privacy by design e la privacy by default. Vediamo di cosa si tratta.

***Le sanzioni**: fino a € 20 milioni per le imprese non facenti parte di gruppi, fino al 4% del fatturato per i Gruppi societari.*

Privacy by design significa che la tutela dei dati personali deve essere pensata e organizzata fin dalla fase progettuale della **raccolta di informazioni**. Diventa obbligatorio prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati. Bisognerà analizzare i flussi di dati connessi all'attività che si vuole effettuare e adottare criteri che **minimizzino i rischi del trattamento e riducano le quantità dei dati trattati** (si parla di minimization of data).

Privacy by default significa che occorrerà **prevenire raccolte di dati non necessari** per le finalità perseguite, evitando di acquisire informazioni eccedenti rispetto agli obiettivi dichiarati nell'informativa.
La privacy quindi diviene il **presupposto** delle attività di trattamento e cessa di essere, come è oggi, un obiettivo secondario da perseguire rispettando adempimenti formali. La privacy cessa di essere un mero requisito legale e diventa un elemento **intrinseco** del processo di gestione delle informazioni.

Questa è **la vera essenza della riforma**. Chi non capisce questo sarà destinato a vagare alla ricerca di un centro di gravità permanente. Privacy by design e by default si fondono in un unico precetto organizzativo che diventa, quindi, la vera stella polare nel cammino verso il corretto trattamento dei dati.

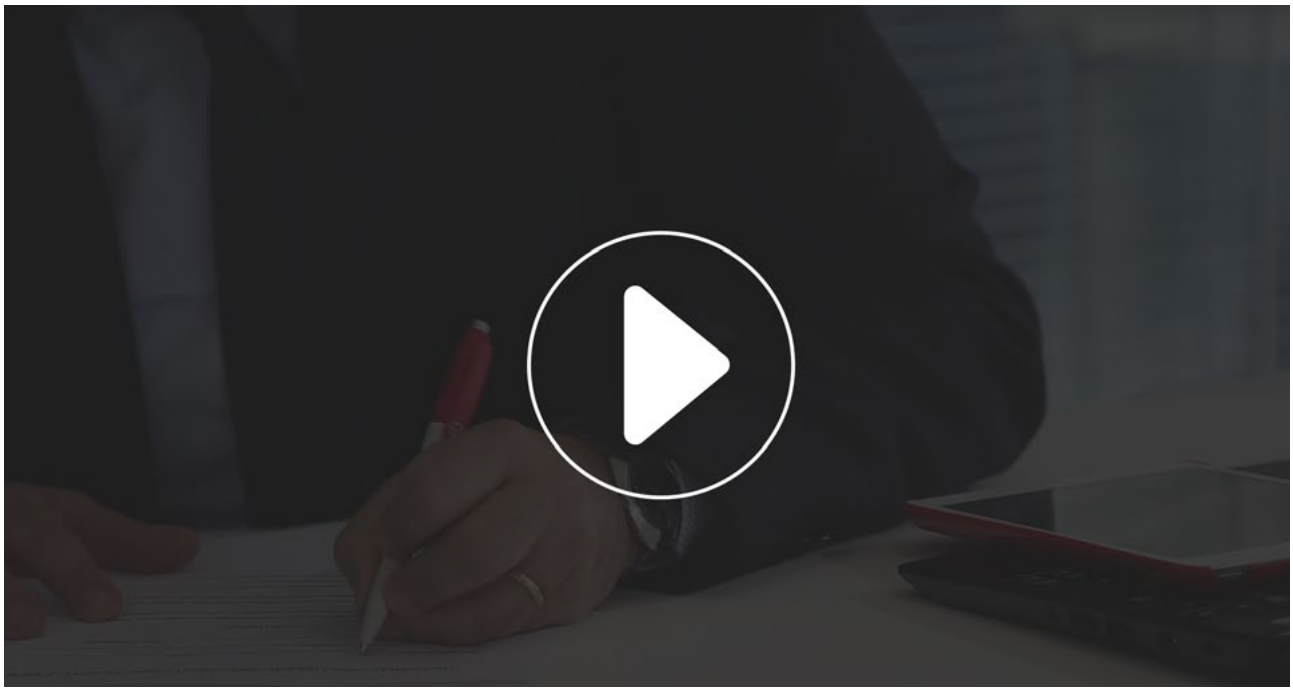
Le **violazioni delle regole** di trattamento dei dati personali danno luogo a conseguenze molto pesanti:

- Fino a € 20.000.000 per i privati e le imprese non facenti parte di gruppi
- Fino al 4% del fatturato complessivo (consolidato) per i gruppi societari

Si tratta di un cambio di passo significativo. Le sanzioni sono pensate per **incidere** sulle condotte dei grandi gruppi multinazionali che trattano dati in diverse aree geografiche e spesso cercano di individuare i **paradisi legali** del trattamento dei dati personali per eludere norme e criteri di comportamento definiti dalle nazioni più rigorose.

Violazione dei dati: quando avviene e cosa fare

CAPITOLO 9



Se non visualizzi correttamente il video, guardalo qui

Secondo il GDPR la «violazione dei dati personali» è la violazione di sicurezza che comporta accidentalmente o in modo illecito la **distruzione**, la **perdita**, la **modifica**, la **divulgazione** non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

In alcuni paesi europei esiste da tempo questa regola, estesa a tutti coloro che trattano dati personali: si parla di **data breach notification**, che è l'obbligo di segnalare all'Autorità le violazioni di dati subite da chi li tratta.

Se in Italia tale obbligo esisteva solo per gli operatori di comunicazioni elettroniche e per poche altre categorie di titolari del trattamento, con la riforma europea tutti dovranno abituarsi a questo **nuovo standard di sicurezza**. Chi tratta dati, in caso di una violazione, dovrà mettere in

atto due differenti azioni:
1. Notificazione della violazione all'Autorità di controllo, entro 72 ore dal fatto
2. Segnalazione al diretto interessato (senza ritardo ingiustificato)

Il mancato rispetto di questo obbligo comporta **sanzioni penali**.

Appare chiaro che questo nuovo standard comporterà interventi significativi per l'adozione di **software di monitoraggio** (comunemente noti come software sentinella) che segnalino immediatamente le violazioni e per l'ottenimento di adeguate **coperture assicurative** che proteggano dai crescenti rischi legati al cosiddetto **cyber risk**.

I fondamentali strumenti per proteggersi dai cyber risk: ***software di monitoraggio e coperture assicurative****.*

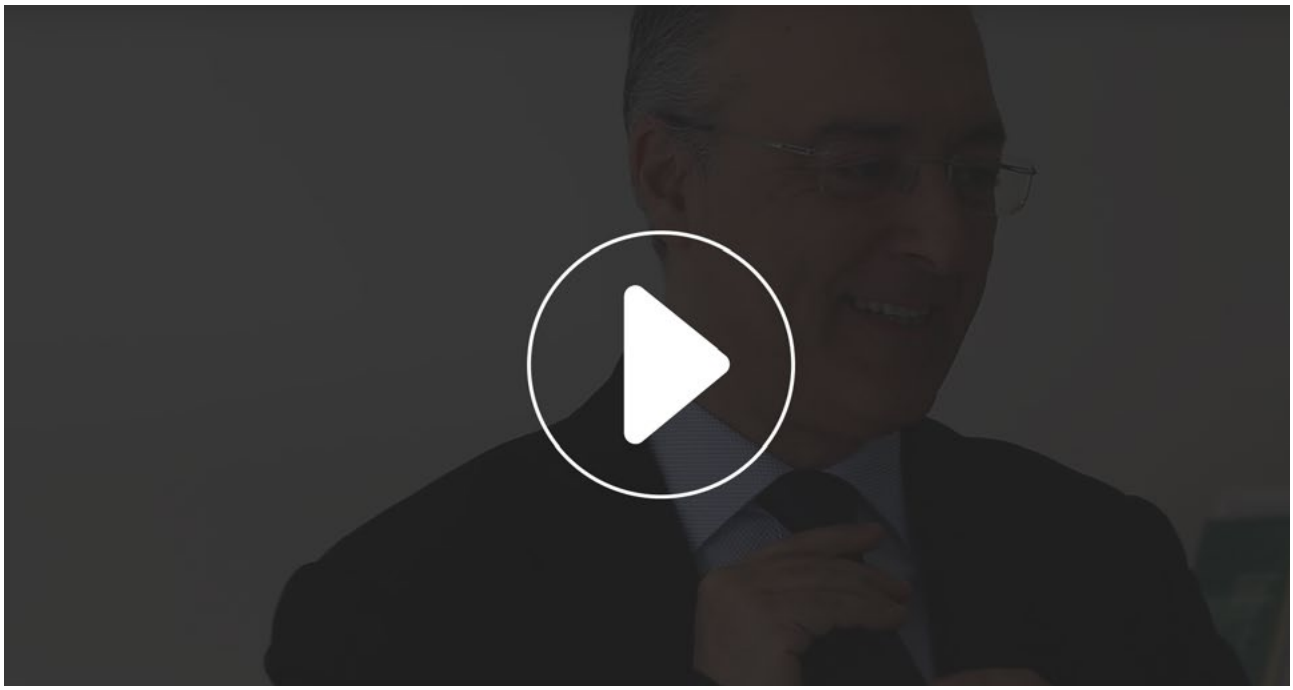
La notifica di violazione deve almeno:

- **Descrivere la natura della violazione** dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione.
- **Comunicare il nome e i dati di contatto** del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni.
- **Descrivere le probabili conseguenze** della violazione dei dati personali.
- **Descrivere le misure** adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Solo se non sia possibile fornire le informazioni contestualmente, sarà possibile fornire questi elementi in fasi successive senza ulteriore ingiustificato ritardo.
È poi l'Autorità a valutare se la violazione vada notificata anche agli interessati.

Portabilità, oblio e limitazione del trattamento

CAPITOLO 10



Se non visualizzi correttamente il video, guardalo qui

Il GDPR conferma tutti i diritti previsti dall'attuale normativa e aggiunge nuove tutele.

In particolare, l'interessato ha il diritto di **accedere ai suoi dati,** cioè ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- **Le finalità** del trattamento.
- **Le categorie di dati** personali in questione.
- **I destinatari** o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali.
- Quando possibile, **il periodo di conservazione** dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.
- **L'esistenza del diritto** dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento.
- **Il diritto di proporre reclamo** a un'autorità di controllo. Qualora i dati non siano raccolti presso l'interessato, tut-

te le informazioni disponibili sulla loro origine.

- **L'esistenza di un processo decisionale automatizzato**, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'interessato ha inoltre il diritto di **rettificare** i dati, ovvero di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'**integrazione** dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

*L'impresa deve garantire all'interessato i diritti all'**accesso**, **rettifica**, **integrazione**, **oblio** e **portabilità** dei propri dati.*

Il testo del Regolamento riconosce nuovi diritti agli interessati. In particolare si fa riferimento a:

- **Diritto all'oblio** (right to be forgotten / right to erasure)
- **Diritto alla portabilità del dato** (data portability)

Il **diritto all'oblio** permette al soggetto interessato di ottenere dal Titolare la **cancellazione di dati personali** che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati, quando:

- I dati non sono più necessari rispetto alle finalità
- L'interessato revoca il consenso
- L'interessato si oppone al trattamento per finalità di marketing
- Il trattamento non è conforme al regolamento

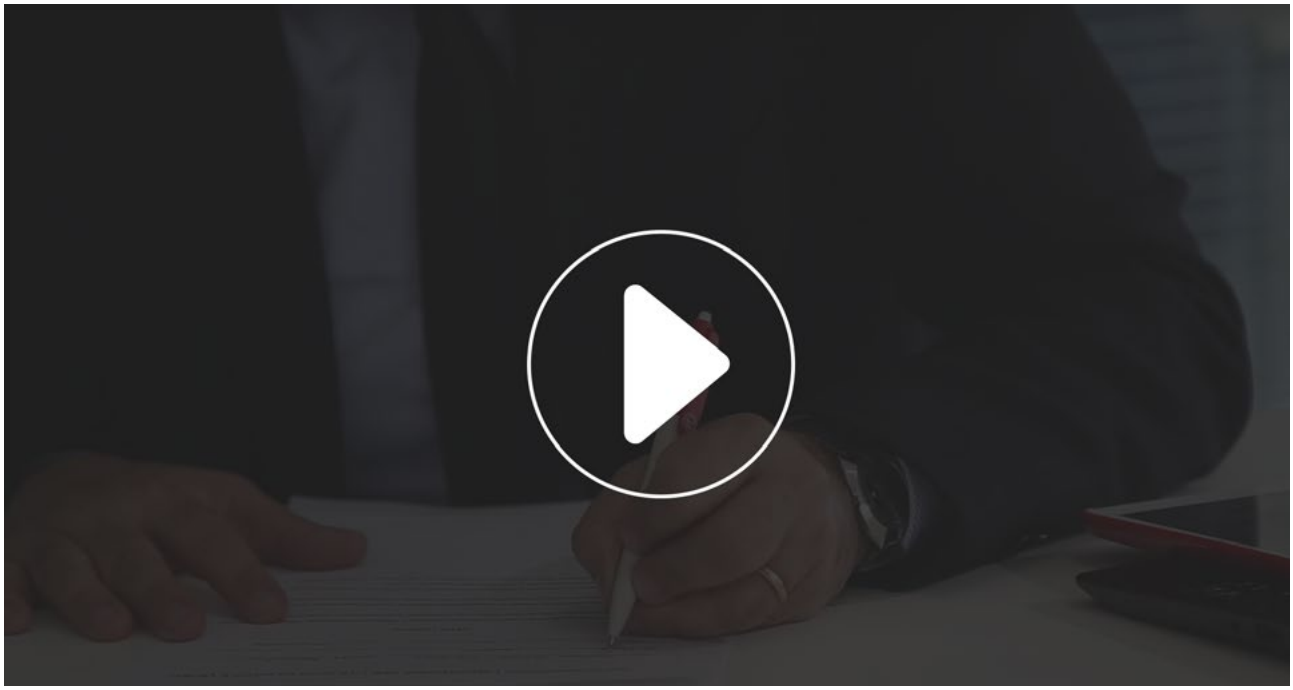
Se il responsabile del trattamento ha reso pubblici i dati, dovrà **adottare tutte le misure ragionevoli**, anche tecniche, per informare i terzi che li stanno trattando, della richiesta dell'interessato al fine di cancellare qualunque link, copia o riproduzione dei suoi dati.

Con **diritto alla portabilità** dei dati si intende il riconoscimento sia del diritto dell'interessato a **trasferire i propri dati** (come quelli del "profilo utente") da un sistema di trattamento elettronico (come il social network) a un altro, senza che il Titolare possa impedirlo, sia del diritto di ottenere gli stessi in un formato elettronico strutturato e di uso comune che consenta di farne ulteriore uso.

Oggi esercitare i diritti di accesso, modifica, integrazione e cancellazione dei dati personali richiede che l'interessato si attivi e superi difficoltà per formulare l'istanza.
I nuovi criteri richiedono invece di prevedere modalità volte ad **agevolare** l'esercizio dei diritti, compresi i meccanismi per richiedere e ottenere gratuitamente l'accesso ai dati, la rettifica e cancellazione. Sarà onere di chi raccoglie i dati predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici.

Come utilizzare i dati ai fini della profilazione

CAPITOLO 11



Se non visualizzi correttamente il video, guardalo qui

Le norme attuali **non definiscono** in cosa consiste la profilazione.

Per molti, basandosi sul significato comune di questa parola, sarebbe profilazione ogni attività di analisi su un database: anche la semplice analisi e clusterizzazione di un database sarebbe profilazione, con la conseguente necessità di dover chiedere un consenso specifico a ogni singolo interessato presente nel database per poter svolgere tale attività.

Il GDPR cambia l'impostazione e finalmente fornisce una **definizione di profilazione**.

È profilazione "**qualsiasi forma di trattamento automatizzato** di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti

riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

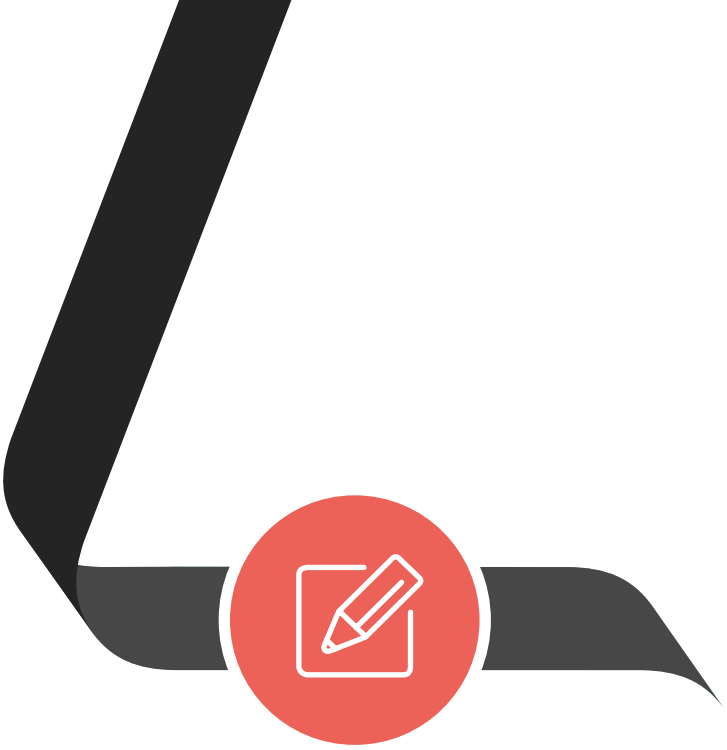
Qualora si effettui profilazione, nasce **l'obbligo di dichiararlo** in modo specifico nell'informativa e di disporre di un **consenso esplicito** dell'interessato. Non basta quindi che la persona manifesti il consenso in modo non equivoco mediante azioni positive: occorre una esplicita manifestazione di volontà.

Questo permette finalmente di disporre di risposte molto precise rispetto agli obblighi da rispettare.

In particolare la riforma chiarisce che la profilazione consiste genericamente in **qualsiasi analisi di dati cui fa seguito un'azione automatica** senza l'intervento dell'uomo. Non si effettua profilazione, quindi, se si analizzano con strumenti informatici i dati presenti nei propri archivi, sottoponendoli alla valutazione preventiva di una persona prima dell'utilizzo, per adattare e verificare i dati stessi. Ne consegue che non occorre un consenso specifico per svolgere tale attività di analisi.

> ***La profilazione è qualsiasi analisi di dati cui fa seguito un'azione automatica**. Per condurla è necessario il consenso esplicito dell'interessato.*

Il consenso esplicito occorre quando si intendono **attribuire profili che determinano azioni automatiche** conseguenti. In definitiva, il GDPR prevede che l'interessato abbia il diritto di non essere sottoposto a decisioni che siano basate unicamente sul trattamento automatizzato, che comportano la sua profilazione, se tale decisione produce effetti che incidono in modo significativo sulla sua persona. Quindi, per valutare se un'attività comporti profilazione occorre anche **soppesare le conseguenze** che l'attribuzione del profilo determina per l'interessato.



Le principali deadline per le aziende

CAPITOLO 12

Il GDPR è pienamente operativo dal **25 maggio 2018**. Entro questa data occorre aver definito tutti gli adempimenti prescritti dalla normativa. E oltre la data occorre manutenere e documentare il processo di gestione delle informazioni. Il trattamento dei dati diventa un processo produttivo da gestire, con fluidità, insieme a tutti gli altri progress aziendali.

Sono tante le attività da svolgere, il che rende consigliabile dotarsi di un modello che consenta di **tenere sotto controllo la compliance** e di essere in grado di dimostrarla.

Ecco la **lista dei doveri** per il Titolare del trattamento.

- **Attribuire** correttamente i ruoli e definire il modello organizzativo di gestione dei dati.
- **Se il trattamento** si basa sul consenso, essere in grado di dimostrare che l'interessato ha concesso il proprio benestare.
- **Se le finalità** del trattamento non richiedono più l'identificazione dell'interessato, non conservare, acquisire o trattare ulteriori informazioni identificative.
- **Adottare** misure appropriate per fornire l'informativa all'interessato.
- **Agevolare** l'esercizio dei suoi diritti.
- **Garantire** all'interessato il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i

dati personali che lo riguardano; osservare il diritto di trasmettere senza impedimenti i dati a un altro titolare.

- **Aderire** ai codici di condotta o a un meccanismo di certificazione per dimostrare il rispetto degli obblighi del titolare.
- **Mettere in atto** misure organizzative per garantire che siano trattati solo i dati necessari alle specifiche finalità del trattamento.
- **Valutare** l'opportunità di utilizzare un meccanismo di certificazione approvato per dimostrare la conformità ai requisiti.
- **Tenere un registro** delle attività di trattamento svolte.
- **Considerare** il rischio per i diritti e le libertà delle persone, al fine di dotarsi di misure tecniche che garantiscano la sicurezza.
- **Far sì** che chiunque agisca sotto l'autorità del Titolare e che nessuno tratti i dati se non istruito.
- **In caso di violazione**, notificarla all'autorità di controllo senza ingiustificato ritardo (ove possibile, entro 72 ore dalla scoperta).
- **Documentare** qualsiasi violazione dei dati personali, circostanze, conseguenze e provvedimenti adottati.
- **Se presenta** un rischio elevato per i diritti e le libertà delle persone, comunicare la violazione all'interessato senza ingiustificato ritardo.
- **Nello svolgere** una valutazione d'impatto, consultarsi con il DPO, qualora sia designato.
- **Raccogliere** le opinioni degli interessati o dei loro rappresentanti, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
- **Prima di procedere** al trattamento, consultare l'autorità di controllo qualora la valutazione d'impatto presenti potenziali rischi elevati in assenza di misure.
- **Ottemperare** all'eventuale parere dell'autorità di controllo.
- **Al momento** di consultare l'autorità di controllo, comunicare tutte le informazioni prescritte.
- **Designare** sistematicamente un Data Protection Officer (DPO) quando necessario.
- **Assicurare** che il DPO sia tempestivamente coinvolto in tutte le questioni riguardanti la protezione dei dati.
- **Sostenere il DPO** nell'esecuzione dei compiti fornendogli le risorse necessarie per mantenere la propria conoscenza specialistica.
- **Non rimuovere** o penalizzare il DPO, e assicurarsi che non riceva alcuna istruzione per l'esecuzione dei propri compiti.
- **Fornire** all'organismo di certificazione tutte le informazioni e l'accesso alle attività di trattamento.
- **Garantire** la conformità al Regolamento.
- **Attestare** nel registro dei trattamenti la valutazione e le garanzie prescritte dal Regolamento.
- **Per essere esonerato** dalla responsabilità, essere in grado di dimostrare che l'evento dannoso non gli è in alcun modo imputabile.
- **Per garantire** che i dati non siano conservati più a lungo del necessario, stabilire un termine per la cancellazione o per la verifica periodica.

Tutte queste attività devono essere oggetto di verifica periodica, da documentare con **cadenza almeno annuale**.

CAPITOLO 13

10 attività per arrivare pronti al GDPR

Rispetto alle norme vigenti in Italia, i campi di maggiore rilevanza introdotti dal GDPR sono:

- Obbligo di definire i **tempi di conservazione** dei dati
- Obbligo di indicare la **provenienza** dei dati in caso di utilizzo
- Obbligo di comunicare tempestivamente al Garante **violazioni** dei propri database
- Obbligo di predisporre il **documento di valutazione di impatto**
- Obbligo di gestire l'**accountability** (prevalentemente mediante il Data Privacy Officer)

Cosa fare, in pratica, per adeguarsi alle novità? Occorre definire un **Privacy Program**, ovvero un processo strutturato di gestione dei dati finalizzato a garantirne un utilizzo controllato.
In generale, nella gestione delle attività di trattamento dei dati entreremo nell'era del Privacy Impact Assessment e del Compliance Risk Management.

È sempre più evidente che i dati personali sono la nuova materia prima che genera il fatturato delle imprese. La materia prima va gestita con **modelli organizzativi evoluti ed efficienti**, comprendendo che si tratta di un tema strategico per le aziende.

*La data protection sarà sempre di più un **fattore competitivo**, e favorirà le aziende che capiranno che non si tratta più solo di una serie di adempimenti da gestire, ma di un processo organizzativo aziendale che ha **natura produttiva** e non solo normativa.*

I PASSI PRELIMINARI DA INTRAPRENDERE

1. *Fare un **inventario** delle proprie informative e verificare come potrebbero cambiare in funzione delle nuove regole. Valutare cosa significa in concreto dover introdurre l'indicazione della fonte dei dati e il tempo di conservazione dei dati.*

2. *Sperimentare nuove forme di informative visuali basate su **icone**.*

3. *Analizzare quali sono i dati di cui si dispone e fare una **mappatura** aggiornata dei dati.*

4. *Dotarsi di **software sentinella** per gestire il nuovo obbligo di notifica delle violazioni nell'uso dei dati personali e verificare l'eventuale flusso extraeuropeo dei dati usando servizi cloud.*

5. *Sperimentare la **privacy by design** e effettuare il **Privacy Impact Assessment**, affidandosi a esperti competenti che aiutino l'azienda a minimizzare gli impatti e a contenere i costi di gestione dei nuovi adempimenti.*

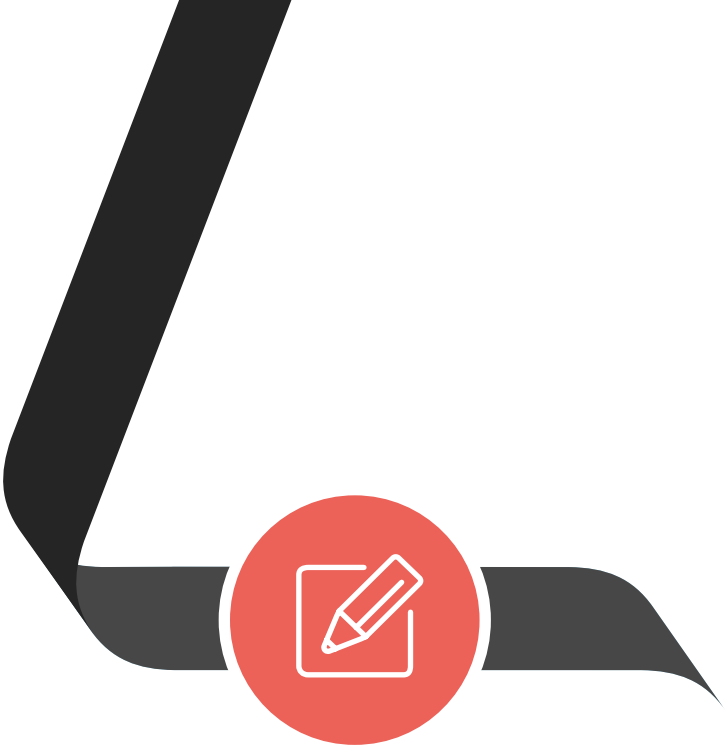
6. *Pensare a come introdurre un **Data Privacy Officer** in azienda.*

7. *Analizzare gli **effetti del diritto alla portabilità** dei dati e adottare **cautele organizzative** per evitare impatti gravi sulla stabilità dei database aziendali.*

8. *Definire le nuove regole di **acquisizione e documentazione del consenso**.*

9. *Verificare con cura i **fornitori dei dati**. Questo è il tempo in cui fare test, test e ancora test.*

10. *Verificare se si trattano dati di **minori** tenendo conto che le nuove regole impongono di gestire anche il consenso degli esercenti la potestà di genitore con il consenso del minore al di sotto dei 16 anni.*



Come dimostrare di essere "privacy compliant"

CAPITOLO 14

Per certificazione si intende l'atto mediante il quale una terza parte indipendente dichiara, con ragionevole attendibilità, che un prodotto, processo o servizio è conforme a requisiti. La certificazione può essere obbligatoria, regolamentata o volontaria.

La **certificazione obbligatoria** riguarda i prodotti che rientrano in specifiche direttive comunitarie le quali forniscono i requisiti minimi per la sicurezza dei lavoratori, dei consumatori e per la tutela dell'ambiente. Il rispetto degli standard di sicurezza, attestato dal marchio CE, è ad esempio condizione essenziale per la commercializzazione dei prodotti nell'ambito dell'Unione Europea.

La **certificazione regolamentata** è quella che fa riferimento a leggi nazionali o regolamenti comunitari. La decisione di aderire a questa certificazione è facoltativa da parte del produttore, ma una volta effettuata la scelta non si può derogare dalla normativa pubblica prevista.

Si parla, invece, di **certificazione volontaria** quando vi è una libera adesione alla certificazione e le norme tecniche non sono riconosciute a livello ufficiale.

La certificazione del trattamento dei dati

personali viene prevista per la prima volta in ambito europeo dal Regolamento 2016/679. **È una certificazione volontaria** che si basa su meccanismi di certificazione della protezione dei dati, nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento. Sono considerate le esigenze specifiche delle micro, piccole e medie imprese.

È poi previsto che oltre all'adesione dei titolari del trattamento o dei responsabili del trattamento, i meccanismi, i sigilli o i marchi possono essere istituiti al fine di **dimostrare la previsione di garanzie appropriate** da parte dei titolari del trattamento o responsabili del trattamento non soggetti a regolamento, in caso di trasferimento di dati fuori dall'UE.
I titolari del trattamento o responsabili del trattamento **assumono l'impegno vincolante e azionabile**, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

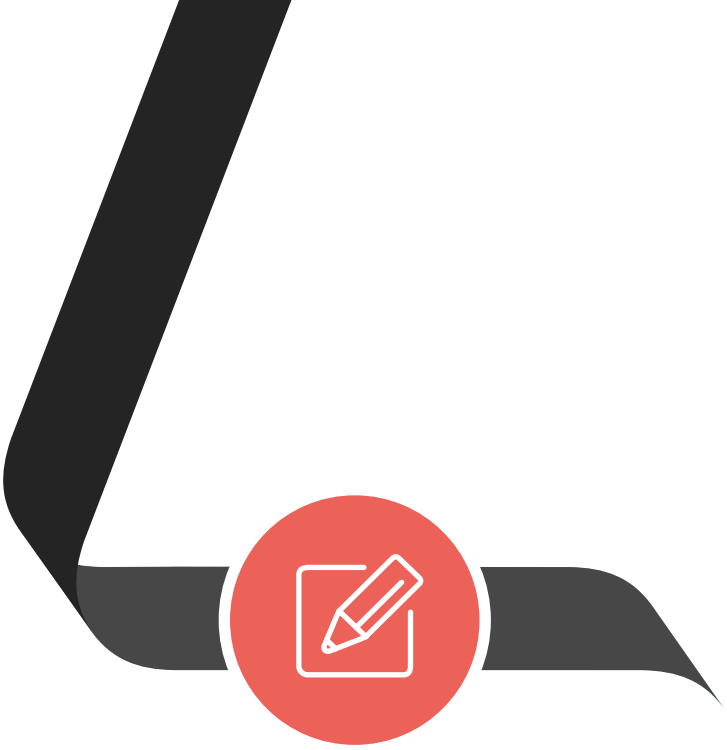
Il GDPR stabilisce che la certificazione è **volontaria** e **accessibile** tramite una procedura trasparente, chiarendo anche che essa non riduce la responsabilità del titolare o del responsabile del trattamento riguardo alla conformità al presente regolamento. Lascia inoltre impregiudicati **i compiti e i poteri delle autorità di controllo** (il Garante per la protezione dei dati personali) di svolgere verifiche e applicare sanzioni in caso di violazioni.

La certificazione è rilasciata al titolare o responsabile per un periodo massimo di 3 anni, può essere rinnovata o revocata.

In base alle norme europee, viene previsto che la certificazione debba essere rilasciata da **organismi di certificazione accreditati** o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente, o dal comitato dei Garanti europei.

La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un **periodo massimo di 3 anni**, e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. La certificazione può essere **revocata** dagli organismi di certificazione o dall'autorità di controllo competente, a seconda dei casi, qualora non siano più soddisfatti i requisiti per la certificazione.

Va detto con chiarezza che la certificazione non riduce la responsabilità del titolare o del responsabile del trattamento e lascia intatti compiti e poteri delle autorità di controllo. Si tratta però di un importante strumento di **verifica imparziale** della conformità dei sistemi di trattamento, favorendo la creazione di un rapporto di fiducia con i soggetti che affidano i loro dati a un titolare o a un responsabile che dispone della certificazione.



Come cambiano i rapporti tra committenti e fornitori

CAPITOLO 15

Il nuovo regolamento europeo comporta molti cambiamenti nei rapporti tra un committente e un fornitore che tratti dati per conto di chi gli affida una determinata attività.

Per i committenti si impone un nuovo **criterio di selezione** dei fornitori, basato sull'affidabilità nel trattamento dei dati personali da parte dei soggetti. Non è più possibile per i committenti scegliere i fornitori con criteri che non tengano conto della **affidabilità** nel trattamento dei dati personali. Il trattamento dei dati personali diventa un elemento da verificare in modo documentato per giustificare la scelta del fornitore.

Secondo le regole attuali, il committente stipula un contratto con il fornitore senza avere l'obbligo di verificare preventivamente le sue modalità di gestione dei dati. Nei contratti di fornitura del servizio si inseriscono clausole che attribuiscono la responsabilità nella gestione dei dati al fornitore.

Questo è un meccanismo di esternalizzazione non solo del servizio, ma anche del **rischio legale** che il servizio comporta. Il fornitore gestisce il servizio con ampia au-

tonomia, eseguendo le istruzioni impartite dal committente (titolare del trattamento). Se viola la normativa **ne risponde direttamente**. Il committente deve solo verificare che il fornitore rispetti le istruzioni impartite e solo in tal caso risponde della violazione.

Per i committenti si impone un nuovo criterio di selezione dei fornitori, basato sull'affidabilità nel trattamento dei dati da parte dei soggetti.

Con il GDPR cambia tutto. Il committente deve effettuare una **valutazione di impatto** nel trattamento dei dati anche quando si avvale di fornitori esterni. Tale valutazione deve prevedere la **scelta del fornitore**. Quindi il Committente deve valutare in anticipo, prima di iniziare il trattamento dei dati mediante un fornitore, se il fornitore selezionato è **adeguato** e dà **garanzie di sicurezza** e buona organizzazione nell'uso dei dati necessari per gestire il trattamento.

Questa valutazione deve essere **documentata per iscritto**. Così impone il nuovo criterio dell'accountability (distribuzione delle responsabilità nel trattamento dei dati documentata e verificata).
Questa è poi una applicazione del nuovo criterio della privacy by design. Se il Committente ha scelto male il Fornitore, senza valutarne l'affidabilità, **ne risponde**.
In sintesi, ecco cosa bisogna fare per trattare correttamente i rapporti con i fornitori che gestiscono dati personali:

- **Documentare** i criteri di scelta dei fornitori.
- **Effettuare** un privacy impact assessment sui trattamenti svolti dai fornitori.
- **Valutare** se i fornitori si sono sottoposti a forme di certificazione sul trattamento dei dati.
- **Gestire** correttamente l'accountability (distribuzione delle responsabilità nel trattamento dei dati documentata e verificata) verso il fornitore.
- **Gestire** correttamente il nuovo criterio della privacy by design.
- **Sottoporre** a verifica periodica (audit) l'attività svolta dal fornitore e documentare tale attività. Se si verificano dei gap, o delle mancanze di conformità documentare tali rilievi e fissare un termine entro il quale porre rimedio a tali carenze.
- **Se i rimedi** non vengono completati entro i termini occorre poter applicare una clausola risolutiva per inadempimento che va prevista nei contratti di fornitura.

Grazie!

PER AVER SCARICATO IL NOSTRO WHITE PAPER

DALLA TEORIA ALLA PRATICA

PROVA MAILUP ORA

Attiva subito la tua piattaforma di Email & SMS Marketing gratuita.
Per 30 giorni puoi usarla senza impegno. Inizia a creare e inviare
campagne dal design d'impatto e ottimizzato per mobile.