

GDPR PROTEZIONE DATI PERSONALI Reg. EU

2016/679



18/10/2026

Perché siamo qui

I principi generali

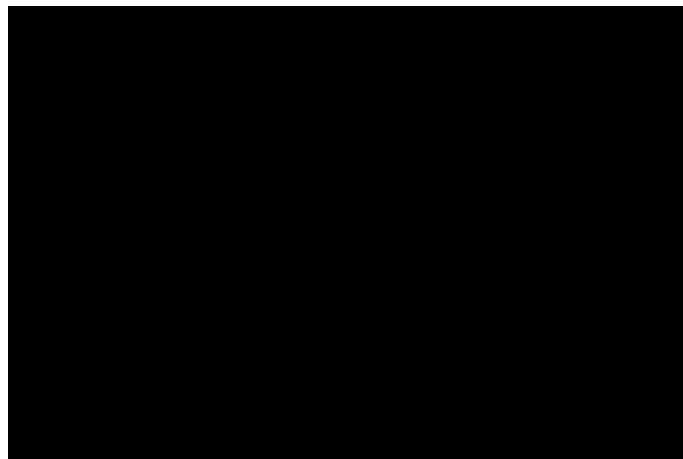
I soggetti del trattamento

Il contesto Ecostampa

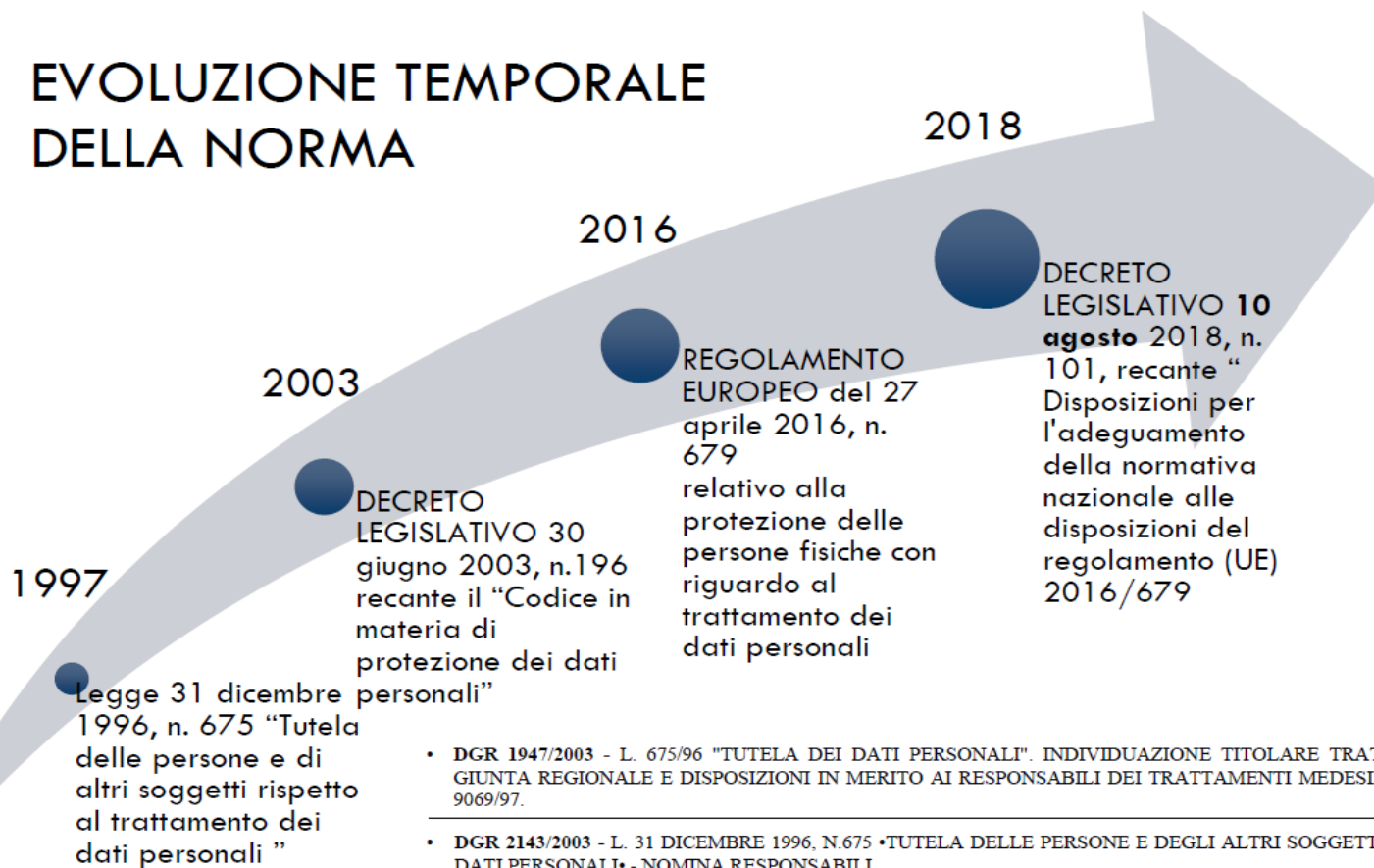




2017-11-25-VIDEO-0
0000507.mp4



EVOLUZIONE TEMPORALE DELLA NORMA



GDPR



I principi generali

*Art. 2: «Il presente regolamento si applica al **trattamento** interamente o parzialmente automatizzato di **dati personali** e al trattamento non automatizzato di dati personali di dati contenuti in un **archivio** o destinati a figurarvi.»*

*Art. 4 : «**trattamento** : qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*

I principi generali

*Art. 4: «**dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;»*

*Art. 4 «**archivio**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico»*

I principi generali

- ***Approccio basato sul rischio** e misure di responsabilizzazione di titolari e responsabili (artt. 23-25).*
- *«Data protection by default and by design»*

***Adozione di comportamenti proattivi** e tali da dimostrare la **concreta** adozione di misure finalizzate ad assicurare l'applicazione del regolamento*

***Analisi preventiva** e un impegno applicativo da parte dei titolari e dei responsabili che devono sostanziarsi in una **serie di attività specifiche e dimostrabili**.*

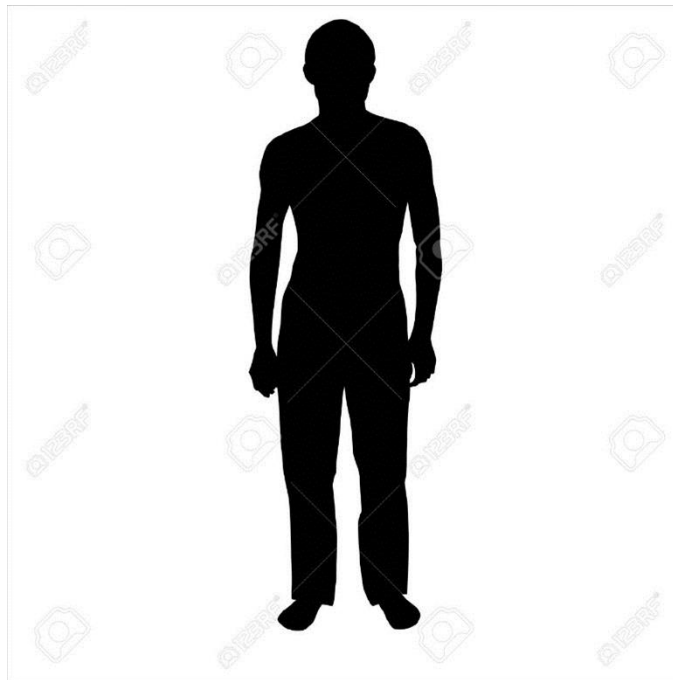
I SOGGETTI DEL TRATTAMENTO.

Il trattamento di dati personali dà luogo ad un rapporto giuridico tra un **soggetto che acquisisce i dati** o svolge altre operazioni sui medesimi e un **soggetto al quale i dati personali si riferiscono**.

D. lgs. 196/2003	Regolamento UE (en)	Regolamento UE (it)
TITOLARE	DATA CONTROLLER	TITOLARE
RESPONSABILE DEL TRATTAMENTO	DATA PROCESSOR	RESPONSABILE DEL TRATTAMENTO
	DATA PROTECTION OFFICER	RESPONSABILE DELLA PROTEZIONE DEI DATI
INCARICATO	DATA HANDLER	ADDETTO AL TRATTAMENTO
INTERESSATO	DATA SUBJECT	INTERESSATO

L'INTERESSATO (Art. 4.1).

La figura dell'interessato è costruita sul concetto di dato personale, per cui ne subisce la forza espansiva. Si deve ritenere che la qualità di interessato cessi con la morte, ossia appunto con il venir meno della persona fisica. La morte tuttavia non fa venire meno il legittimo interesse degli eredi, ad avere accesso a informazioni del deceduto e dunque a far valere disposizioni regolamentari relative a dati riferibili a quest'ultimo.



TITOLARE DEL TRATTAMENTO (Art. 4.7 e 24)

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. È il centro di imputazione delle decisioni sulle finalità e sui mezzi del trattamento.

POTERI	OBBLIGHI
- Decide su finalità, mezzi e sulla sicurezza	- Obblighi e adempimenti in materia di sicurezza: 1. decide e programma le misure di sicurezza, adotta tecniche di privacy by design e by default, procede alla valutazione d'impatto e alla consultazione preventiva; 2. attua le misure di sicurezza dotandosi di policy interne e codici di condotta; 3. si attiene ai doveri di correttezza, trasparenza e di accountability; 4. sceglie i soggetti che ricoprono ruoli subalterni.
- Può individuare all'interno della propria struttura ruoli subordinati a cui affidare operazioni di trattamento, istruendoli adeguatamente.	- Obblighi di garanzia nei confronti dell'interessato
- Può autorizzare i responsabili a designare altri responsabili.	- Obblighi di collaborazione con soggetti preposti al controllo.

TITOLARE DEL TRATTAMENTO (Art. 4.7 e 24)

Il titolare del trattamento è, dunque, il soggetto che:

Assume le decisioni relative alle finalità del trattamento.

Impartisce istruzioni e direttive vincolanti nei confronti dei responsabili.

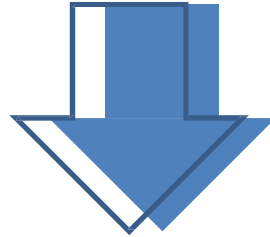
Svolge funzioni di controllo rispetto all'operato dei responsabili.



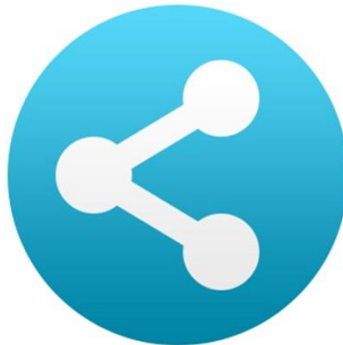
CONTITOLARE DEL TRATTAMENTO (Art. 26).

Laddove due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolare del trattamento.

La contitolarità va intesa, dunque, nel senso di co-decisione in merito alle finalità e ai mezzi.



I contitolari sono obbligati a istituire un accordo di riparto (a forma libera) che deve riflettere in modo puntuale i ruoli reciproci, il riparto degli obblighi previsti dal Regolamento, il rapporto reciproco nei confronti degli interessati.



Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Il Responsabile del trattamento o chiunque agisca sotto la sua autorità, non può trattare dati personali a cui ha accesso se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Il Responsabile del trattamento deve essere nominato dal titolare o da altro Responsabile previa autorizzazione scritta del titolare, specifica o generale. La designazione avviene per contratto o altro atto giuridico.

OBBLIGATORIA.

Se il titolare decide di esternalizzare il trattamento

FACOLTATIVA.

Se il Responsabile è nominato da altro responsabile.

RESPONSABILE DEL TRATTAMENTO (Art. 4.8 e 28).

ELEMENTI DI SUBORDINAZIONE NEL TRATTAMENTO DEI DATI	OBBLIGHI E ADEMPIMENTI
- Ha il dovere di agire secondo le istruzioni di trattamento fornite dal titolare ed impartirle in senso conforme ai suoi dipendenti e collaboratori che accedano a dati personali forniti dal titolare.	- Deve assistere il titolare, se richiesto, nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una valutazione d'impatto sulla protezione dei dati e dalla previa consultazione dell'Autorità garante.
- Risponde del danno causato dal trattamento solo se non ha adempiuto gli obblighi del Regolamento specificamente diretti ai responsabili o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento	- Deve collaborare con il Garante e con gli organismi indipendenti di certificazione.
- Se fa proprie le finalità e i mezzi viene considerato come un titolare, determinando l'applicazione delle disposizioni relative	- Presta supporto al data protection officer fornendogli i mezzi, delle informazioni e degli accessi necessari a realizzare la sua attività, pur senza interferire con l'istruzione nello svolgimento dei suoi compiti.

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

- a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

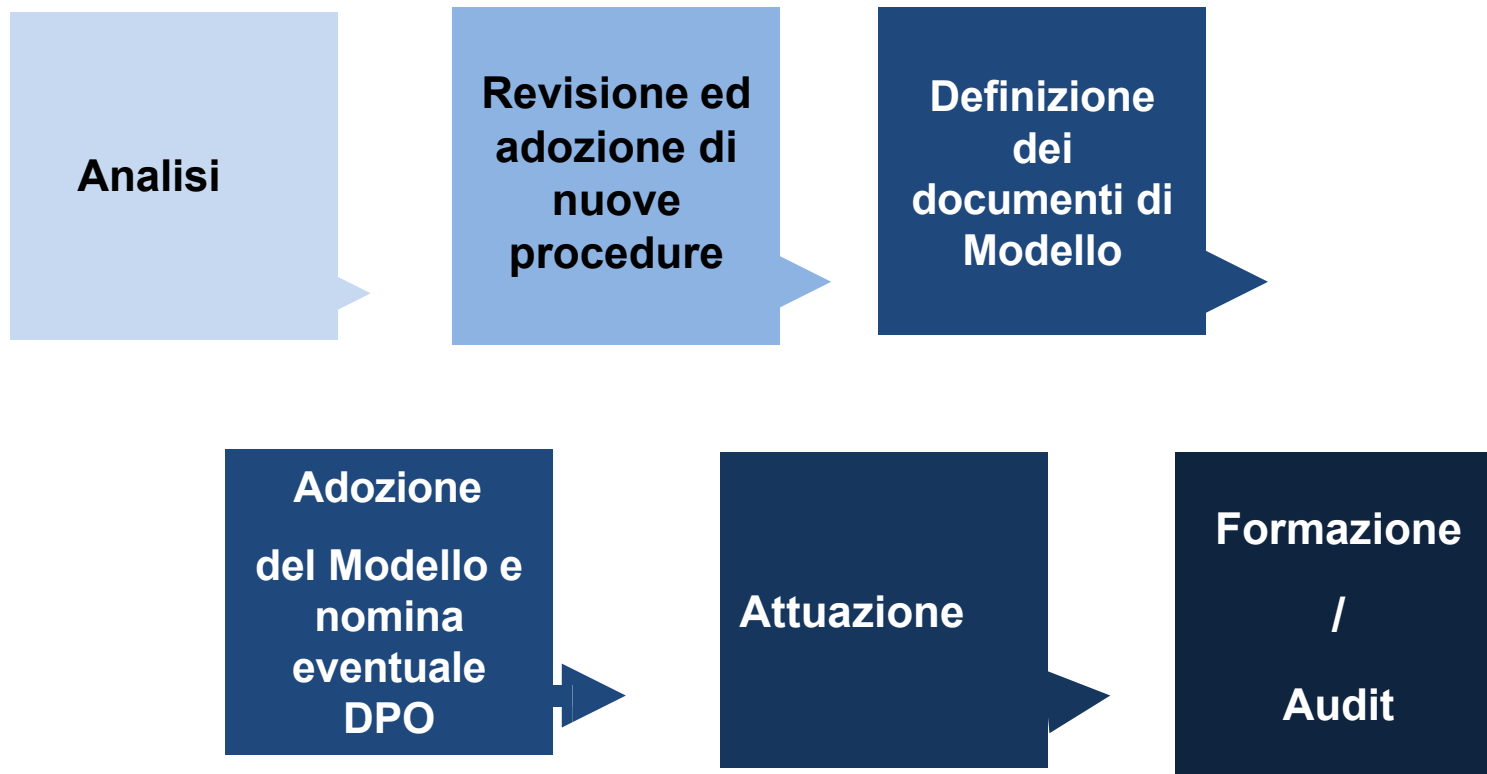
1. **sensibilizzare e consigliare** il Titolare in merito agli obblighi (misure e procedure tecniche e organizzative) derivanti dal Regolamento;
2. **sorvegliare** sull'applicazione delle regole di trattamento compresa l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e l'effettuazione degli audit connessi;
3. **sorvegliare** sull'applicazione del Regolamento, con particolare riguardo alla protezione fin dalla progettazione, alla protezione di default, alla sicurezza dei dati, alle informazioni dell'interessato ed alle richieste degli stessi per esercitare i diritti riconosciuti;
4. **controllare** che il Titolare effettui la Valutazione d'impatto sulla protezione dei dati (c.d. DPIA) e richieda all'Autorità di Controllo l'autorizzazione preventiva o la consultazione preventiva nei casi previsti;
5. **fungere** da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento e consultarla, se del caso, di propria iniziativa;
6. **informare** i rappresentanti del personale (es. rappresentanti sindacali) sui trattamenti che riguardano i dipendenti.

PER ESSERE *COMPLIANT* AL REGOLAMENTO SI DOVRA' ...

✓ Adottare MODELLI ORGANIZZATIVI analoghi a quelli utilizzati nell'applicazione del D.Lgs. 231/2001

✓ Dotarsi, ove necessario o ritenuto opportuno, del Responsabile per la tutela dei dati personali (*Data Privacy Officer* – DPO)

PROCESSO PER L'ADOZIONE DI UN MODELLO ORGANIZZATIVO *PRIVACY*



COMPLIANCE - ANALISI

**mappatura dei trattamenti
(finalità,
comunicazione/diffusione,
conservazione e trasferimento
internazionale dei dati, ecc.)**

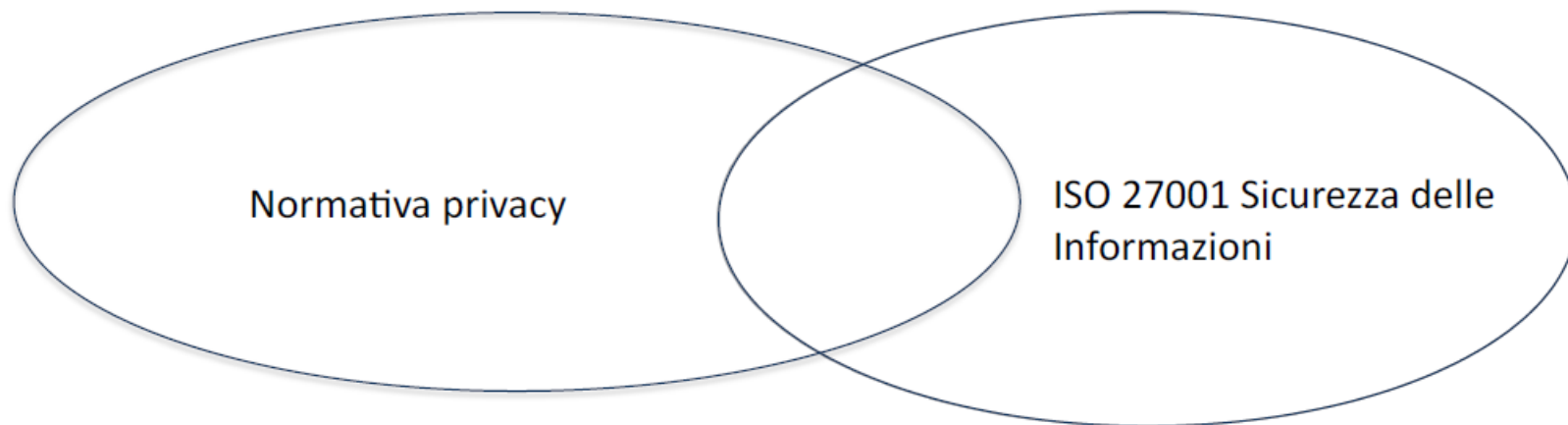
**censimento delle banche dati
(categorie degli interessati,
natura dei dati, ecc.)**

ubicazione delle banche dati

**distribuzione dei compiti e delle
responsabilità**

Quanto già fatto, in termini di “processo”, sul tema ISO 27001

Protezione dei dati personali e sicurezza delle informazioni



La normativa della protezione dei dati personali è fortemente interconnessa con lo standard ISO/IEC 27001. Lo stesso Garante ha contribuito a questo allineamento (Provvedimento generale sulla biometria e Parere sul sistema informativo nazionale della fiscalità).

Quanto già fatto, in termini di “processo”, sul tema ISO 27001

GESTIONE DEL RISCHIO

I PASSI DELLA VALUTAZIONE DEL RISCHIO

1. Individuare il contesto
2. Definire l'ambito della valutazione del rischio
3. Definire la politica di sicurezza delle informazioni
4. Identificare gli asset
5. Identificare i proprietari dei rischi
6. Identificare e determinare la verosimiglianza delle minacce
7. Identificare e valutare le vulnerabilità
8. Valutare le conseguenze
9. Stimare il livello di rischio
10. Ponderare il rischio è accettabile

GESTIONE DEL RISCHIO ESEMPIO DI CALCOLO DEL RISCHIO

$$R = I \times P$$

I = impatto (da 1 a 3)

P = probabilità (da 1 a 3)

R = rischio (da 1 a 9)

Probabilità	Impatto		
	Basso (1)	Medio (2)	Alto (3)
Alta (3)	Medio $1 \times 3 = 3$	Alto $2 \times 3 = 6$	Alto $3 \times 3 = 9$
Media (2)	Basso $1 \times 2 = 2$	Medio $2 \times 2 = 4$	Alto $3 \times 2 = 6$
Bassa (1)	Basso $1 \times 1 = 1$	Basso $2 \times 1 = 2$	Medio $3 \times 1 = 3$

Scala del Rischio: Alto (> 5), Medio (> 3 sino a 5), Basso (da 1 sino a 2),

Multe fino a

**€20
milioni**

di euro oppure il 4% del
volume d'affari globale
annuo di un'azienda

Grazie per l'attenzione!

