



**RISK SOLVER**

Gdpr - Cyber - Life Protection





## Chi è RISK SOLVER

*Risk Solver si occupa di ricerca, identificazione, sviluppo e distribuzione di soluzioni innovative per la gestione integrata dei rischi emergenti.*

*Il Risk Management attuato non si limita all'identificazione dei rischi stessi, ma al loro approccio, mitigazione e risoluzione.*

*La nostra metodologia integra diverse componenti e competenze: analisi dei singoli mercati, affiancamento alle diverse realtà aziendali private e pubbliche, identificazione dei players più qualificati, costruzione di soluzioni multidisciplinari che portino ad una corretta gestione dei rischi, comprensivi di strategie e soluzioni articolate, fino ad arrivare alla tutela assicurativa personalizzata.*

*L'expertise dei professionisti, interni ed esterni, il continuo dialogo con le Aziende, da un lato, ed i partners specializzati nei vari ambiti, dall'altro, consentono un risk management attivo che non si limita alla "rincorsa del problema" ma, al contrario, ne prevede l'impatto e ne risolve le conseguenze.*

*I recenti e impattanti cambiamenti normativi europei in ambito privacy (GDPR 2016/679) ci vedono da tempo coinvolti nella creazione di soluzioni uniche ed articolate in linea con le mutate esigenze.*





## Il Regolamento UE 2016/679

in vigore dal 24 Maggio 2016

*Il regolamento 2016/679 è entrato in vigore il 24 maggio 2016 e vedrà la sua totale e completa applicazione dal 25 maggio 2018.*

*È obbligatorio in tutti i suoi elementi e direttamente applicabile in tutti gli Stati membri (art. 99).*

*Interessa qualsiasi soggetto: aziende di ogni ordine e grado, enti pubblici e individui che debbano acquisire, gestire, conservare, trasferire ovvero trattare dati personali.*

*Si applica anche qualora il trattamento dei dati personali di cittadini UE venga effettuato in Stati extra-UE.*

*Alcuni stati tra cui la Svizzera si sono già adeguati al regolamento per poter operare nel contesto europeo.*

*La precedente direttiva 95/46/CE viene abrogata e sostituita dal nuovo regolamento europeo 2016/679 (art. 94).*



## Finalità e obiettivi del regolamento UE 2016/679

*In sintesi quanto richiesto dal regolamento GDPR*

1. *obbliga le aziende a creare ed adottare una propria Privacy by Design e/o Privacy by Default*
2. *Adottare in tutte le aziende pubbliche e private il **registro delle attività***
3. *Introduce nuovi diritti per gli interessati quali il **Diritto all'Oblio** e la **Portabilità dei Dati Personali***
4. *Valutare il rischio relativamente all'adozione di un nuovo trattamento dei Dati Personali (**PIA**)*
5. *Verificare periodicamente i livelli di sicurezza e protezione dei Dati Personali trattati (**Data Breach**)*
6. *Il regolamento introduce la figura del **DPO (Data Protection Officer)***



## Finalità e obiettivi

### Privacy by Design (art. 25)

*I titolari e i responsabili del trattamento devono mettere in atto misure tecniche ed organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati, assolvendo ai principi di diligenza.*

#### Tutto ciò richiede:

- ▶ *Una precisa analisi (PIA) per valutare le singole realtà di partenza*
- ▶ *Identificazione di adeguate strategie di intervento*
- ▶ *Identificazione e adozione delle soluzioni idonee*



## Finalità e obiettivi

### Privacy by Default (art. 25)

*La privacy by default presuppone invece che i titolari e i responsabili del trattamento dei dati, nella modalità operativa del trattamento, adottino misure e soluzioni tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.*

#### Tutto ciò richiede che:

► *le aziende e le pubbliche amministrazioni abbiano un approccio alla protezione dei dati personali **proattivo e non più reattivo**, rendendo necessario prevedere modalità operative, configurazioni e misure di sicurezza in grado di salvaguardare la riservatezza, l'integrità e la disponibilità dei dati personali (RID) "by default", ovvero nel momento in cui essi "entrano" nell'organizzazione.*



## Finalità e obiettivi

### Data Breach (artt. 32, 33 e 34)

*I titolari del trattamento dei dati devono adottare misure idonee al fine di garantire l'integrità, la disponibilità e la riservatezza dei Dati Personali.*

#### Tutto ciò richiede che:

- ▶ *I dati personali siano limitati ad ogni specifica finalità del trattamento e per il tempo strettamente necessario al trattamento, definendo di conseguenza il periodo di conservazione e l'accessibilità agli stessi, evitando eccessi e ridondanze*
- ▶ *Obbligo di indagine che comprende: la sorgente da cui è partita la violazione, le modalità di aggressione, il tipo di dati violati, i soggetti che sono stati coinvolti, ciò che l'Azienda attuerà al fine di evitare il ripetersi di questa tipologia di attacco*
- ▶ *Obbligo di denuncia alle autorità competenti entro le 72 ore e di notifica a tutti i contatti i cui dati siano o possano essere stati violati, nel minor tempo possibile.*





## Le sanzioni previste

*Sono state definiti i limiti generali sanzionatori che saranno applicati ogni qualvolta vengano rilevate delle irregolarità nel trattamento dei dati personali*

### ► Riguardanti i dati Comuni

Sanzioni fino a € 10.000.000  
oppure estensibile fino al 2% del  
fatturato lordo se superiore alla  
sanzione, per ogni violazione

### ► Riguardanti i dati sensibili e giudiziari

Sanzioni fino a € 20.000.000  
oppure estensibile fino al 4% del  
fatturato se superiore alla  
sanzione, per ogni violazione

*La sanzione viene calcolata sulla base del fatturato lordo dell'Azienda se singola, del Gruppo se facente parte di un Gruppo, mondiale in caso di Multinazionale.*





## Le soluzioni Risk Solver

Risk Solver supporta Aziende, enti pubblici e professionisti in questo necessario passaggio di adeguamento al GDPR, introducendo **soluzioni uniche ed innovative** che si basano su :

- ▶ **Analisi del rischio dal punto di vista legale, informatico, assicurativo e reputazionale**
- ▶ *Utilizzo di strumenti tecnici di analisi, controllo e reportistica per assolvere alle richieste del regolamento*
- ▶ *Definizione della soluzione AD HOC da adottare in funzione delle singole necessità*
- ▶ **Adeguamenti logistici, tecnici e formativi** *costituenti le misure minime richieste dalla normativa vigente*
- ▶ *Applicazione di meccanismi di certificazione dei processi*
- ▶ *Introduzione di strumenti di e-learning evoluta per gli utenti dei sistemi informativi aziendali*

**Il tutto con il supporto di esclusive soluzioni assicurative** che garantiscono, in caso di **Data Breach**, supporto di tipo legale, informatico e reputazionale, così da contenere l'impatto economico conseguente agli **effetti negativi** di un attacco.



## Pre-assessment legale - tecnologico/ assicurativo - reputazionale

Il servizio di analisi legale effettua, tramite un pre-assessment documentale, una puntuale verifica al fine di determinare l'effettivo posizionamento dell'azienda rispetto a quanto previsto dal regolamento.

L'approfondita analisi tecnologica, grazie a uno specifico e articolato pre-assessment,

consente un preciso calcolo dei rischi informatici dell'impresa rispetto a possibili attacchi e obblighi normativi.

La componente reputazionale, consente di definire e dimensionare questo rischio in funzione della tipologia dell'azienda e dei conseguenti rischi di perdita di fatturato.

Tutto ciò permette di definire un benchmark di riferimento di partenza e concordare con l'Azienda gli obiettivi da raggiungere.



**RISK SOLVER**

Insurance & Technical Section  
SEZIONE E: Dati

1. Conservate o processate alcuno dei seguenti tipi di dati sensibili di consumatori? N° approx. di records

(a) Informazioni finanziarie (inclusi dati su carte di credito o debito) SÌ  NO

(b) Informazioni medico / sanitarie SÌ  NO

(c) Informazioni sull'identità (inclusi codici fiscali, dettagli dei passaporti, etc.) SÌ  NO

(d) Nomi, indirizzi e numeri di telefono SÌ  NO

2. Conservate o processate alcuno dei seguenti tipi di dati sensibili di aziende? N° approx. di records

(a) Proprietà intellettuale riservata / segreti industriali SÌ  NO

(b) Informazioni finanziarie SÌ  NO

3. Utilizzate la crittografia nei seguenti scenari?

(a) I dati sensibili memorizzati nel vostro sistema sono criptati? SÌ  NO

(b) I dati sensibili sono criptati sui nastri/dischi di backup? SÌ  NO

(c) I dati sensibili sono criptati quando trasmessi al di fuori del vostro sistema? SÌ  NO

(d) I dati sensibili sono criptati quando trasferiti su dispositivi portatili (USBs, Laptops, etc)? SÌ  NO

Se No, ad alcuna delle domande sopra riportate, fornire commenti riguardo eventuali azioni per mitigare i rischi

4. Sminimizzate i dati per ridurre il rischio di perdita su base scala in caso di sinistri informatici? SÌ  NO

**RISK SOLVER**

ver. 10-17

Gdpr - Cyber - Life Protection

11



## Approccio basato su modello di Risk Management e Compliance

*Le risposte fornite dalle aziende alle domande del pre-assessment vengono elaborate da una evoluta piattaforma di Enterprise Risk Management proprietaria. L'utilizzo di questa piattaforma software consente una valutazione immediata di Risk Scoring fornendo gli indici di rischio su tre livelli :*

- 1. Situazione aziendale generale*
- 2. Situazione aziendale per aree: legale, tecnologica, assicurativa, cyber e reputazionale*
- 3. Situazione aziendale di dettaglio relativamente ad ogni singola domanda contenuta nei questionari*

*L'analisi del rischio si basa sulle linee guida ed i principi della norma UNI ISO 31000 e su algoritmi per la verifica della conformità alla normativa 196/03, al regolamento UE 2016/679, alle sanzioni economiche e penali, alla adeguatezza delle difese contro attacchi cyber.*



# Enterprise Risk Management Framework

La piattaforma software analizza ogni singolo dato inserito e genera un report sia in formato grafico, rappresentato dalla mappa di calore, sia in formato numerico con i relativi indici di rischio.

Queste informazioni permettono di individuare con maggior precisione le aree più critiche sulle quali intervenire con priorità per abbattere più rapidamente il rischio.



Risk Category	Risk Factor	RF Risk
Informazioni generali	Rischi per PDP legati alla gestione di personale	0.226
	Rischi per PDP legati al sito web	0.215
	Rischi per PDP legati a reti, IT, relativi, budget, DDP/BCP	0.196
Informazioni generali	Rischi per PDP legati alla gestione di dati	0.343
	Rischi per PDP legati ai siti e procedure esterne utenti	0.308
Rischi legati agli aspetti legati al trattamento in relazione ai dati	Rischi in Informative	0.292
	Pre-disposizione Liste attori trattamento	0.398
Rischi legati agli aspetti procedure di gestione in relazione ai dati	Rischi gestione del consenso	0.608
	Pre-disposizione Liste attori trattamento	0.487
Rischi in relazione ai dati	Rischi in gestione dei dati per non IT	0.257
	Rischi in gestione dei dati per non IT	0.257

Le tabelle precedenti, che forniscono graduatorie analitiche del rischio, vengono sintetizzate nel grafico di seguito.

Risk Classification	Risk Value (%)
Rischio Medio Globale secondo criteri CRSA	35.17%

Risk Category	Risk Factor	Question	Probability	Impact	Risk
Informazioni generali	Informazioni generali	L'azienda è iscritta a qualche albo o associazione professionale?	Likely	Marginal	0.021
		La società possiede alcun tipo di accreditamento professionale?	Likely	Marginal	0.021
		Avete una persona dedicata responsabile della sicurezza informatica e Privacy?	Remote	Marginal	0.04
		Effettuate sempre un controllo delle referenze per tutti i dipendenti ed amministratori che hanno accesso ai dati sensibili?	Likely	Marginal	0.021
		Effettuate sempre un controllo delle referenze per tutti i dipendenti ed amministratori del vostro personale in possesso di accesso ai dati sensibili?	Remote	Marginal	0.04
		Limitate l'accesso ai dati sensibili (inclusi i dati fisici) solamente a chi ne ha fatto specifica richiesta?	Remote	Marginal	0.04
		Avete una procedura che impedisca l'accesso ai sistemi da parte di ex dipendenti entro 60 giorni dalla cessazione del rapporto lavorativo?	Remote	Marginal	0.04
		Avete procedure di sicurezza scritte che vengono riviste annualmente e approvate dai vostri utenti/amministratori/colleghi clienti di distribuzione dati. Sono stati i vostri contatti con dipendenti del settore IT negli ultimi 12 mesi?	Likely	Marginal	0.021
		Ci sono contatti che sono stati interessati a causa di comportamenti disonesti o fraudolenti?	Remote	Critical	0.08
		Esiste ed è regolarmente mantenuto un elenco dei siti Web e dei visitatori (URL)?	Remote	Critical	0.08
Rischi per PDP legati alla gestione di dati	Rischi per PDP legati alla gestione di dati	I vostri siti web sono di fatto dei "basic brochure website"?	Occasional	Marginal	0.021
		I vostri siti web contengono materiale pubblicitario di soggetti terzi?	Occasional	Marginal	0.021
		I vostri siti web prevedono contenuti creati dagli utenti (Chat rooms, bacheca, forum di discussione, ecc)?	Occasional	Marginal	0.021
		I vostri siti web contengono grossi volumi di contenuti pubblicati?	Occasional	Marginal	0.021
		I vostri siti web consentono il download / streaming di contenuti multimediali?	Occasional	Marginal	0.021
		I vostri siti web prevedono un'area di login per gli utenti?	Occasional	Marginal	0.021
		Pubblicate contenuti di soggetti terzi nei vostri siti web?	Occasional	Marginal	0.021
		Se sì, avete procedure in essere per garantire il rispetto dei diritti all'utilizzo di tali contenuti?	Occasional	Marginal	0.021
		È consentito a soggetti terzi di caricare commenti o contenuti direttamente sul vostro sito web?	Occasional	Marginal	0.021
		Se sì, viene offerta la possibilità ai visitatori del sito di segnalare contenuti inappropriati?	Occasional	Marginal	0.021
Avete stimato la percentuale del vostro fatturato derivante da attività online o di automazione?	Occasional	Marginal	0.021		

## Strumenti informatici di analisi e controllo

*Le soluzioni tecnologiche forniscono una continua valutazione, controllo e reportistiche del rischio informatico.*

*Le funzionalità, costantemente adeguate ed aggiornate, ed ulteriormente implementabili su richiesta del cliente, già oggi garantiscono:*

- ▶ *Analisi e monitoraggio delle attività sul mondo web (rischi esterni)*
- ▶ *Verifica della presenza di duplicazioni di dati personali in azienda (rischio interno)*
- ▶ *Analisi delle abitudini comportamentali degli utenti*
- ▶ *Rilevamento di attività sospette (attacchi, comportamenti anomali di utenti, sistemi infetti)*
- ▶ *Pannello di controllo e alert, reportistica periodica relativamente ad anomalie della rete aziendale*

*Grazie a questi strumenti l'Azienda avrà **consapevolezza dei rischi** della propria rete, possibilità di verificare dimostrare l'efficacia delle misure tecniche adottate per la protezione dei dati personali.*



## Soluzioni tecnologiche

*Risk Solver fornisce le soluzioni tecnologiche indirizzate a singoli client, alle piccole reti (tipicamente per Piccole Imprese e Professionisti), alle medie e grandi reti aziendali, grazie a un insieme di strumenti sia proprietari, sia di terze parti.*

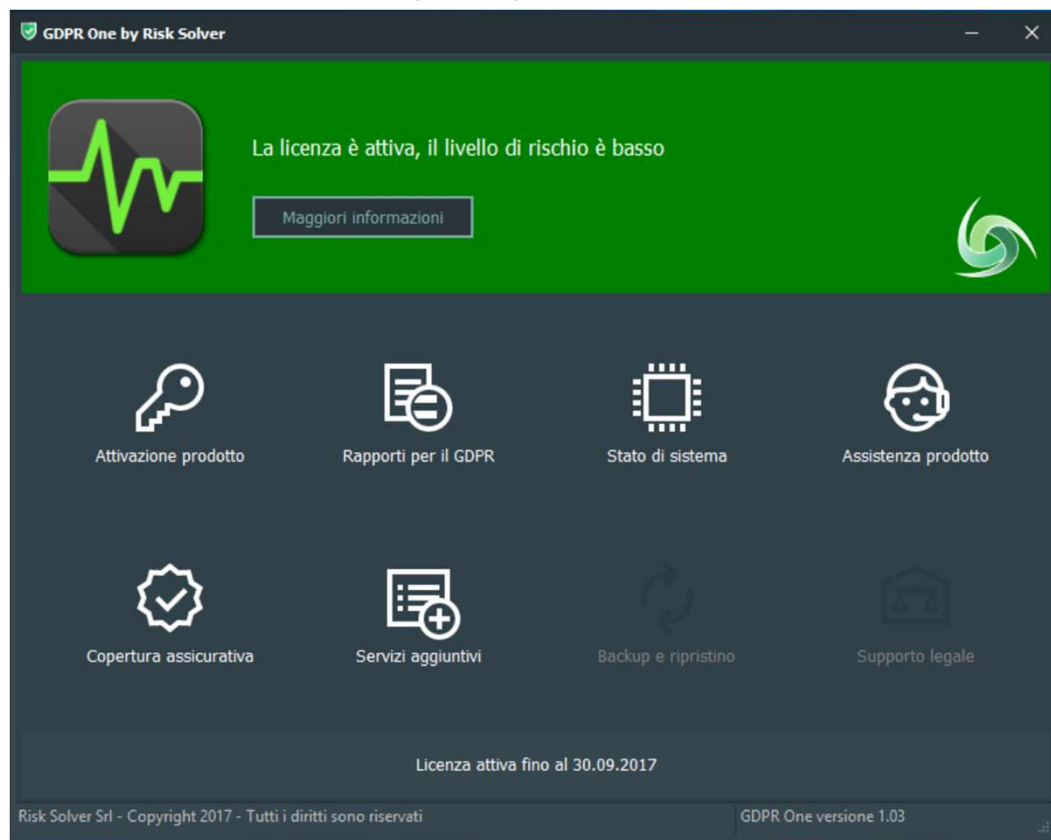
*Le funzionalità, costantemente adeguate ed aggiornate, ed ulteriormente implementabili su richiesta del cliente garantiscono:*

- ▶ *Progettazione e realizzazione sui concetti di Privacy by Design e By Default*
- ▶ *Strumenti per hardware e software inventory, data mapping, crittografia e pseudonimizzazione*
- ▶ *Aggiornamento costante dei Sistemi Operativi e dei principali Sw di utilizzo quotidiano*
- ▶ *Innalzamento dei livelli di sicurezza grazie a riconfigurazione accurata dei Sw di base, introduzione di GPO*
- ▶ *Reportistica relativa alle misure previste ed adottate per dimostrare la conformità al regolamento (Accountability)*
- ▶ *Notifica di attività sospette (attacchi, accessi non autorizzati, etc.) per tutelare il titolare ed il responsabile del trattamento*
- ▶ *Registrazione dei Log di Sistema e archiviazione su piattaforma di conservazione a norma*

*Grazie agli strumenti adottati, i Professionisti, le PMI oltre ad avere **consapevolezza dei rischi** sui propri computer, sono in grado di verificare e dimostrare l'adozione misure tecniche adeguate e conformi al regolamento.*



## GDPR One - il servizio per piccole aziende e studi professionali



**RISK SOLVER**

ver. 10-17



Gdpr - Cyber - Life Protection



# GDPR One - il servizio per piccole aziende e studi professionali

**Stato di sistema**

Aggiornamento programmi | Manutenzione registro e GPO | Gestione utenti | Protezione sistema | Realtime Monitor

Stato dei database | Conservazione dati di sistema | Firewall | Regole di sicurezza

### Aggiornamento dei database

Come impostazione di default, GDPR One controlla periodicamente la presenza di aggiornamenti nel proprio database on-line di minacce, scaricandoli automaticamente e installandoli in background. E' possibile eseguire manualmente un aggiornamento del database in qualsiasi momento.

Ultimo aggiornamento: **26.09.2017 16:22:46**

Esegui l'aggiornamento ora

Risk Solver Srl - Copyright 2017 - Tutti i diritti sono riservati | GDPR One versione 1.03

**Stato di sistema**

Aggiornamento programmi | Manutenzione registro e GPO | Gestione utenti | Protezione sistema | Realtime Monitor

Stato dei database | Conservazione dati di sistema | Firewall | Regole di sicurezza

### La conservazione remota è attiva

Come da normativa GDPR, tutti i file che contengono una descrizione degli eventi successi nel sistema, deve essere conservato in un formato protetto presso un archivio elettronico sicuro. La banca dati di GDPR One si occupa di mantenere tutte queste informazioni in una cassaforte digitale presso un datacenter certificato. I files conservati non contengono informazioni personali o sensibili.

Ultimo allineamento: **5 settembre 2017 alle 18:25**

Data	File	Descrizione
<u>Log di Windows</u>		
05 settembre 2017	Applicazione	Log delle applicazioni proveniente dal registro di windows
05 settembre 2017	Sicurezza	Log sugli eventi inerenti la sicurezza di sistema
05 settembre 2017	Installazione	Log provenienti dalle installazioni di software nel sistema
05 settembre 2017	Sistema	Log generali di sistema
05 settembre 2017	Eventi inoltrati	Log degli eventi provenienti da sistemi collegati
05 settembre 2017	Eventi hardware	Log degli eventi hardware di sistema
05 settembre 2017	Winsock	Log degli eventi provenienti da Winsock
<u>Log applicazioni</u>		

Risk Solver Srl - Copyright 2017 - Tutti i diritti sono riservati | GDPR One versione 1.03

RISK SOLVER

ver. 10-17



Gdpr - Cyber - Life Protection

## Soluzioni di Cyber Security

*Il rischio Cyber si posiziona oggi ai massimi livelli tra i rischi che le aziende devono contrastare.*

*Purtroppo diventa sempre più evidente come le strategie tradizionali di mitigazione del rischio cyber si rivelino inefficienti.*

*Invece Risk Solver, grazie alla rete di esperti (con oltre ventennale esperienza) in cyber security e alla collaborazione con un primario centro di ricerca internazionale, sviluppa per le aziende programmi innovativi di Cyber security uniti a metodologie di Risk Management.*

*La nostra metodologia si compone di attività*

- ▶ *Cyber risk analysis e servizi di consulenza in Cyber Security*
- ▶ *Proactive Vulnerability Assessment*
- ▶ *Applicazione di GPO derivanti da standard governativi/militari*
- ▶ *Network e System penetration test (inclusi human test)*



## Registro dei trattamenti e dei consensi

*Il software in cloud per consentire una gestione semplificata e informatizzata degli adempimenti normativi, ed in particolare consente implementazione del registro dei Trattamenti e del registro dei consensi, documentazione*

- ▶ *Gestione Multi Azienda (per gestire organizzazioni aziendali complesse)*
- ▶ *Multi Account per consentire la gestione delle attività da parte di un team di utenti*
- ▶ *Accountability (Gestione della documentazione, delle nomine: incaricati, responsabili, titolari, DPO)*
- ▶ *Attraverso interfaccia utente agevola una completa compilazione del Registro dei Trattamenti*
- ▶ *Descrizione delle misure tecniche adottate a fronte dei rischi rilevati dagli strumenti di analisi utilizzati da Risk Solver*
- ▶ *Implementazione del registro dei consensi per calendarizzare tutte le attività*
- ▶ *Pannello di gestione del Data Breach per gestire la descrizione e la denuncia alle autorità competenti*



## Formazione per utenti e professionisti

*Innovativi servizi di e-learning e di e-testing basati su piattaforme sviluppate AD-HOC  
Per rendere più fruibile il servizio e più efficace la formazione.*

*Il nostro obiettivo è di rendere accessibile l'apprendimento grazie a tecnologie di  
e-learning altamente avanzate che si basano su Learning Management System di ultima  
generazione.*

- ▶ *Contenuti multimediali interattivi*
- ▶ *Sistema di certificazione delle competenze*
- ▶ *Percorsi didattici in base al livello di apprendimento*
- ▶ *Istruzione dei collaboratori su procedure e processi aziendali*

*l'utilizzo del protocollo SCORM (Shareable Content Object Reference Model) permette di certificare la formazione*



## Data Protection Officer

*Il DPO non è una novità assoluta nel panorama legislativo europeo, tuttavia con il Regolamento 2016/679 diventa una figura fondamentale per l'azienda per tutte le scelte relative all'organizzazione aziendale e agli strumenti tecnici, relativamente al Trattamento dei dati. Il DPO è un professionista con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati e con competenze tecniche.*

*I dati di contatto del DPO devono essere pubblicati e resi noti agli interessati oltre ad essere comunicati all'autorità di controllo competente.*

*Il DPO può essere un dipendente del titolare del trattamento dei dati oppure può essere un libero Professionista, esterno e autonomo, ingaggiato in base a un contratto di servizio.*

*In qualunque caso il lavoro del DPO deve svolgersi in assoluta autonomia e indipendenza: nessuno può dargli alcuna istruzione circa l'esecuzione dei suoi compiti e il responsabile della protezione dati non può svolgere altre mansioni o compiti in conflitto di interessi con quelle proprie del DPO, essendo tenuto in ogni caso al segreto e alla riservatezza in ordine alle sue funzioni di responsabile della protezione.*

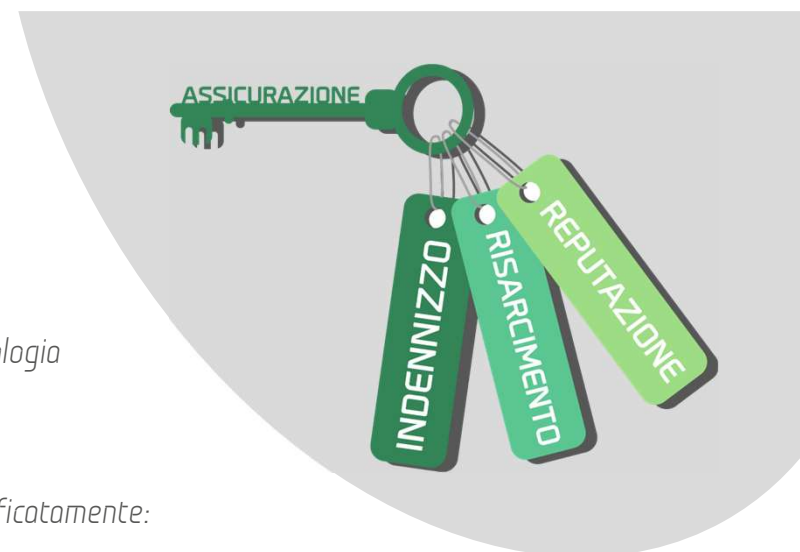


## Le soluzioni assicurative

*Le soluzioni assicurative, esclusive ed articolate, vengono create **AD HOC** sulla base dei pre-assessments legali, informatici e reputazionali, effettuati in partenza e dei successivi adeguamenti e adattamenti, in funzione della tipologia di rischio dell'Azienda Cliente.*

*Le soluzioni assicurative garantite da Risk Solver permettono di proteggere il patrimonio aziendale grazie alle sue innovative coperture, che coprono specificatamente:*

- ▶ Spese legali
- ▶ Spese di indagine
- ▶ Spese per il recupero dell'immagine
- ▶ Risarcitorie: danni verso terzi
- ▶ Indennizzanti : fermo attività, ripristino sistemi, recupero/ricostruzione dati, e così via



## Le Certificazioni

*L'adesione ad uno schema di certificazione accreditato (ISO 17065) è rivolta a tutte le aziende che trattano dati personali.*

*I meccanismi di certificazione forniscono i principi e le linee di controllo per una completa valutazione della conformità dei processi interni all'organizzazione in merito alla protezione dei dati personali, tenendo in particolare considerazione la gestione dei rischi.*

*Essi definiscono i controlli di sicurezza perchè i dati rispettino sempre i requisiti di esattezza, accuratezza, attualità, coerenza, completezza, credibilità e aggiornamento, richiesti dal regolamento.*

*È necessario scegliere uno schema applicabile a qualsiasi Titolare del trattamento, qualunque sia il settore di appartenenza e che si adatti al tipo di trattamento realizzato e che risponda ai requisiti previsti dal GDPR nella sua applicazione in tutti gli Stati membri,*

*Deve inoltre essere adeguato agli eventuali criteri integrativi di cui agli artt. 42 e 43 del Reg. 2016/679, quando questi verranno rilasciati dal comitato o dall'autorità nazionale competente ai sensi degli artt. 55 e 56, essendo ancora in fase di definizione.*



grazie per la vostra attenzione

email: [info@risksolver.it](mailto:info@risksolver.it)  
P.IVA 09938980969  
n.ro REA 2123490  
Iscrizione RUI N. B000579737



Sede Legale Via G. Saragat, 10/C - 20128 - Milano  
Ufficio di Milano Via Del Carmine, 8 - 20121 - Milano  
Ufficio di Roma: Via Anagnina 314 - 00173 - Roma  
Ufficio di Palermo: Via XX Settembre 68, 90141 - Palermo