REGOLAMENTO EUROPEO

SULLA TUTELA DEI DATI PESONALI (UE 2016/679)

MYWAY SECURITY SOLUTIONS

PIU' DIRITTI E PIU' OPPORTUNITA' PER TUTTI

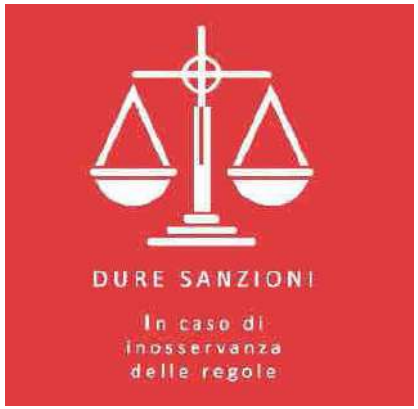
Il Regolamento risponde alle sfide poste dagli **sviluppi tecnologici** e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali dei cittadini dei Paesi dell'Unione Europea.

Le innovazioni non riguardano solo le persone fisiche ma anche le **aziende**, gli **enti pubblici**, le **associazioni** e i **liberi professionisti**.

MYWAY SECURITY SOLUTIONS

DURE SANZIONI

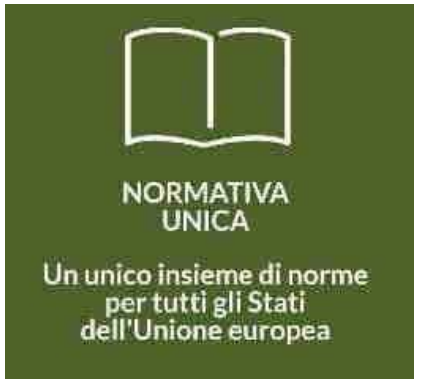
Multe fino a **20 mln €** oppure al **4% del fatturato di gruppo**, se superiore



APPLICABILITA'

Anche alle **imprese non UE** che trattano dati di persone in UE.

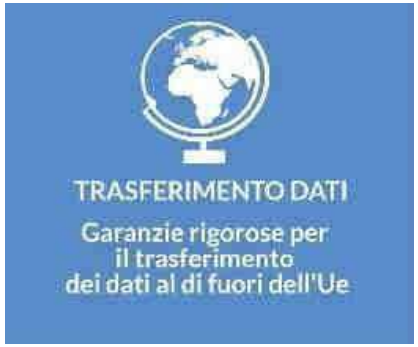
Dal **25 maggio 2018** per **tutti gli Stati UE**



MYWAY SECURITY SOLUTIONS

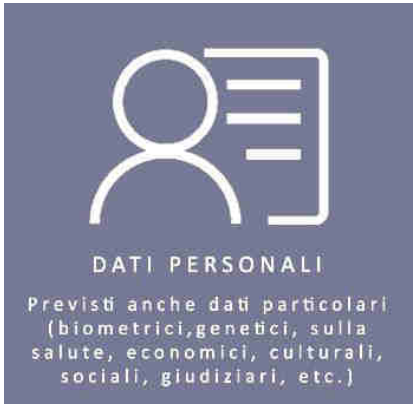
TRASFERIMENTO DATI FUORI UE

Sempre sottoposto a regolamentazione UE **come oggi**



DATI PERSONALI

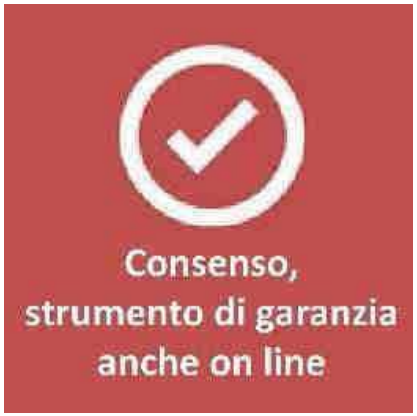
Definizione più ampia che include: dati **genetici,** sulla **salute fisica e mentale, biometrici, economici, identità sociale e culturale, giudiziari.**



MYWAY SECURITY SOLUTIONS

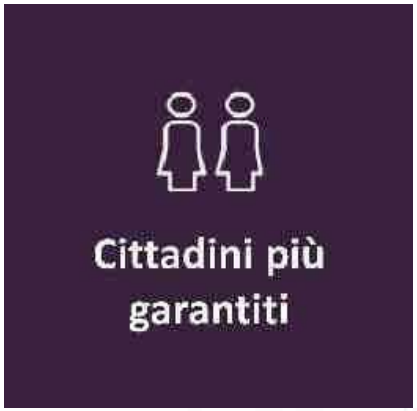
CONSENSO

Il consenso al trattamento deve essere **preventivo, inequivocabile** ed avvenire in modo **esplicito**



MINORI

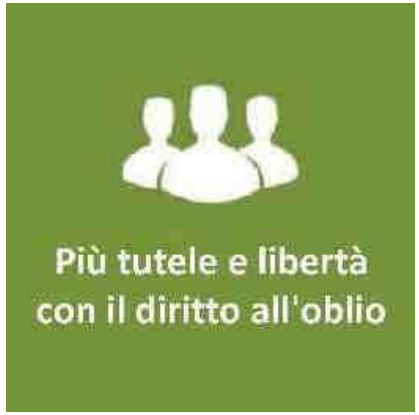
Occorre il **consenso dei genitori** per il trattamento dei dati dei minori di **16 anni**



MYWAY
SECURITY SOLUTIONS

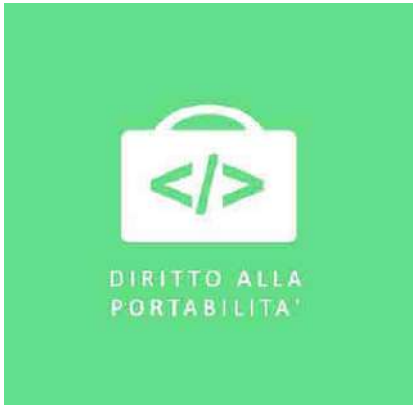
DIRITTO ALL'OBLIO

Si potrà ottenere la **cancellazione dei propri dati personali**, anche on line, se, ad esempio, non sono più necessari o sono stati trattati illecitamente



DIRITTO ALLA PORTABILITA'

Gli utenti possono richiedere una **copia dei dati personali** in un formato facilmente trasferibile



MYWAY
SECURITY SOLUTIONS

DPO

La nomina di un **Data Protection Officer** è obbligatoria per le imprese che processano elevati volumi di dati e consigliabile per le altre

PIA

I progetti con **rischi elevati** per i dati personali dovranno essere sottoposti ad un **Privacy Impact Assessment**

MYWAY
SECURITY SOLUTIONS

PRIVACY BY DESIGN

Prodotti, sistemi e processi devono **prevedere** la tutela dai dati personali **già dalla progettazione**

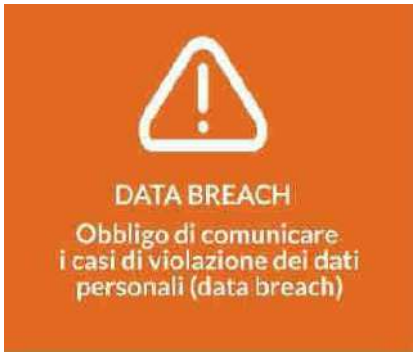
PRIVACY BY DEFAULT

Pe impostazione predefinita si tratteranno **solo i dati personali indispensabili** e solo per il **periodo strettamente necessario**

MYWAY
SECURITY SOLUTIONS

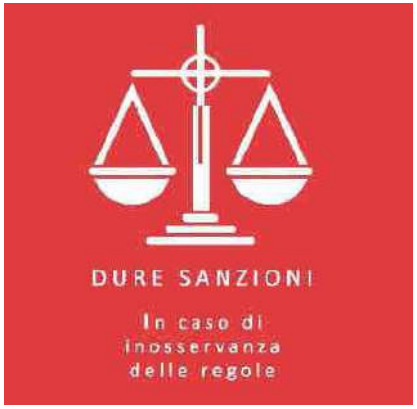
DATA BREACH

Il Titolare deve **comunicare una violazione entro 72 h** dall'evidenza, se il rischio per gli interessati è elevato



TITOLARE E RESPONSABILE TRATTAMENTO DATI

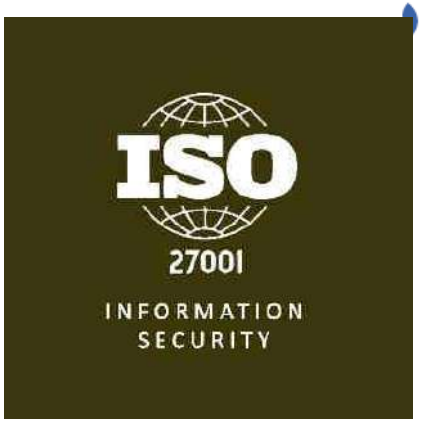
Il rapporto tra Titolare e Responsabile deve essere regolato tramite **apposito contratto**.



Titolare e Responsabile sono **responsabili in solido**

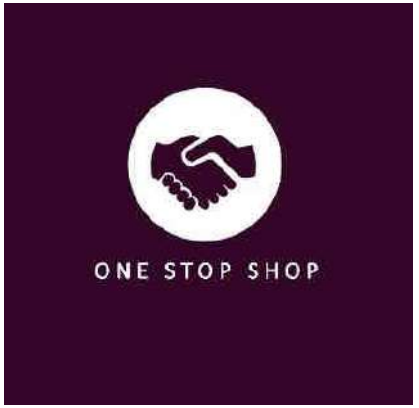
MYWAY
SECURITY SOLUTIONS

CERTIFICAZIONI E CODICI DI CONDOTTA



ISO 27001, altre certificazioni e codici di condotta aiutano a **dimostrare** che le **misure tecniche** ed **organizzative sono adeguate**

ONE STOP SHOP



Le organizzazioni internazionali potranno **comunicare con una sola Autorità** per tutti i paesi in cui operano

MYWAY
SECURITY SOLUTIONS

GLI EFFETTI
PER LE IMPRESE

SANZIONI AMMINISTRATIVE

ART 83

SE TITOLARE E RESPONSABILE
NON ADEMPIONO AGLI OBBLIGHI

- ACCORDO CON CONTITOLARI
- MISURE DI SICUREZZA
- NOTIFICA E COMUNICAZION E VIOLAZIONE DATI
- VALUTAZIONE IMPATTO PRIVACY ECC.

FINO A **10 MLN** €

o **2%** DEL **FATTURATO DI GRUPPO**, SE MAGGIORE

MYWAY SECURITY SOLUTIONS

SANZIONI AMMINISTRATIVE

ART 83

IN CASO DI VIOLAZIONE DELLE SEGUENTI DISPOSIZIONI

- Principi di base del trattamento e consenso
- Diritti dell'interessato
- Trasferimento dei dati verso Paesi terzi o organizzazioni internazionali
- Mancata osservanza di un ordine dell'Autorità di controllo (es. limitazione di trattamento, sospensione dei flussi di dati, (etc.)

FINO A **20 MLN €**

o **4%** DEL **FATTURATO DI GRUPPO**, SE MAGGIORE

MYWAY SECURITY SOLUTIONS

SANZIONI PENALI

ART 84

Gli **Stati membri stabiliscono le norme relative alle altre sanzioni** per le violazioni del Regolamento e, in particolare, per le violazioni non soggette a sanzioni amministrative pecuniarie

ACCOUNTABILITY

RESPONSABILITA' DEL TITOLARE DEL TRATTAMENTO DATI

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli interessati, il Titolare del trattamento mette in atto **misure tecniche e organizzative adeguate per garantire,** ed essere in grado di ***dimostrare*****,** che il **trattamento è effettuato conformemente al regolamento**. Le misure sono riesaminate e aggiornate qualora necessario.

REGISTRO DEI TRATTAMENTI

Contenente i dati del/dei Titolare/i e degli eventuali Responsabili, le **finalità del trattamento**, una descrizione delle categorie di **interessati** e dei dati personali, eventuali **trasferimenti** verso **paesi terzi** ed una descrizione generale delle **misure di sicurezza**. Deve essere messo **a disposizione del Garante** e manutenuto sia dal Titolare che dagli eventuali Responsabili. I registri sono tenuti in **forma scritta**.

I **destinatari**, gli

DATA PROTECTION BY DESIGN

DATA PROTECTION BY DEFAULT

Le misure a protezione di dati devono essere **adottate** già al momento della **progettazione** di un prodotto, di un processo o di un software.

Il Titolare del trattamento deve mettere in atto **misure tecniche e organizzative adeguate** per garantire in ogni caso che siano trattati solo i dati necessari per ogni specifica finalità.

RESPONSABILITÀ IN SOLIDO DI TITOLARE E RESPONSABILE.

Il Titolare e il Responsabile del trattamento sono **responsabili in solido** nei confronti dell'interessato, per un eventuale danno causato dal trattamento.

DATA BREACH

VIOLAZIONE DEI DATI

Nel caso si verifichino violazioni di dati personali, il Titolare ne deve dare **comunicazione all'Autorità di Controllo** (entro 72 ore) e, nei casi più gravi, anche agli interessati avviene solo per violazione di dati biometrici).

VALUTAZIONE DI IMPATTO

PRIVACY IMPACT ASSESSMENT - PIA

Sostituisce la notificazione. È la **valutazione preliminare dei rischi e degli impatti** a cui andrebbe incontro un processo qualora dovessero essere violate le misure di protezione dei dati. Prevede attività come la **mappatura** dei dati e dei trattamenti, la **pianificazione** degli **interventi tecnologici e organizzativi** di protezione dei dati ed una valutazione complessiva di **riduzione dello stato di rischio**.

CERTIFICAZIONI

Il Titolare potrà far certificare i propri trattamenti (es. **ISO 27001**), in misura **parziale o totale**, anche ai fini di trasferimenti di dati in **Paesi terzi**. L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi positivi per la **riduzione delle sanzioni** o per la **valutazione della correttezza delle procedure** da parte dell'Autorità di Controllo.

DIRITTO ALL'OBLIO

DIRITTO ALLA PORTABILITA' DEI DATI

OBLIO: diritto di ottenere la **cancellazione dei dati** di un interessato purché non sussistano motivi legittimi per conservarli.

PORTABILITA': possibilità per l'interessato di **ricevere i propri** dati personali in un formato strutturato, leggibile da dispositivo automatico e di uso comune e di ottenere, salvo impedimenti tecnici, la trasmissione diretta dei dati **da un Titolare all'altro**.

RESPONSABILE PROTEZIONE DATI

DATA PROTECTION OFFICER - DPO

Figura indipendente nominata da titolare e dal responsabile del trattamento

Informa e consiglia

Sorveglia

Fornisce un parere sulla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento

E' punto di contatto e collabora l'Autorità di controllo

Valuta i rischi del trattamento, considerandone la natura, il campo di applicazione, il contesto e le finalità

Figura di vigilanza, interna o esterna

Designato in base a qualità professionali

E' coinvolto in tutte le questioni

Non deve ricevere istruzioni e non dev'essere in conflitto d'interessi

OBBLIGATORIO PER

Pubbliche amministrazioni e organismi pubblici

Soggetti che effettuano un controllo regolare e sistematico degli interessati su larga scala

Soggetti che trattano, su larga scala, dati particolari

MYWAY SECURITY SOLUTIONS

VALUTAZIONE D'IMPATTO

PRIVACY IMPACT ANALYSIS – PIA

- Descrizione sistematica dei trattamenti previsti e delle finalità del trattamento
- Valutazione necessità e proporzionalità dei trattamenti in relazione alle finalità
- Valutazione dei rischi per i diritti e le libertà degli interessati
- Descrizione delle misure previste per affrontare i rischi

OBBLIGATORIA IN CASO DI
(Sostituisce la notificazione del trattamento ex Codice Privacy)

- Uso di nuove tecnologie con rischio per interessati
- Profilazione
- Categorie particolari di dati su larga scala
- Sorveglianza su larga scala

Larga scala = big data: notevole quantità di dati personali a livello regionale, nazionale o sovranazionale

MYWAY SECURITY SOLUTIONS

SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto, delle finalità del trattamento e dei rischi (probabilità e impatto) per i diritti e le libertà degli interessati

TITOLARE
RESPONSABILE

DEVONO METTERE IN ATTO **MISURE TECNICHE E ORGANIZZATIVE APPROPRIATE** PER GARANTIRE UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO

MISURE TECNICHE

Pseudonimizzazione

Cifratura

Anonimizzazione

MISURE ORGANIZZATIVE

Provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali

Ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico

Come si valuta l'adeguatezza?
Si considerano i rischi derivanti da:

Distruzione, perdita, modifica, divulgazione non autorizzata, accesso, accidentale o illegale dati personali trasmessi, memorizzati o comunque trattati

DATA BREACH

COMUNICAZIONE DI VIOLAZIONE DEI DATI

Il titolare del trattamento notifica la violazione all'autorità di controllo competente [...] Senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato non è richiesta se il titolare:

Ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura

Ha successivamente adottato misure atte a sopraggiungere di un rischio elevato per i diritti e interessati

MYWAY SECURITY SOLUTIONS

IL NOSTRO APPROCCIO PER L'ADEGUAMENTO AL GDPR 629/2016

1. **Consulenza Legale e Organizzativa**
2. **PIA Privacy Impact Assessment**
3. **Data Protection BY DESIGN e BY DEFAULT**
4. **Data Protection Officer**
5. **Disaster recovery e Business Continuity**
6. **la formazione sulla Sicurezza logica**
7. **il Sistema Gestione della Privacy**
8. **la certificazione ISO 27001**
9. **la Sicurezza logica**
10. **l'assicurazione Cyber risk**

MYWAY SECURITY SOLUTIONS

I SERVIZI DI MY WAY DEDICATI AL TRATTAMENTO DEI RISCHI

- QUICK AUDIT
- PREVENZIONE (ANALISI)
- GESTIONE (SOLUZIONI)
- TRASFERIMENTO DEI RISCHI RESIDUI (AL MERCATO ASSICURATIVO)

QUICK AUDIT
(pre-analisi)

Rapido ma intenso.

Condotto dai nostri esperti (in organizzazione, information security e aspetti legali).

Parte dall'analisi della documentazione disponibile e da interviste alle funzioni aziendali coinvolte (marketing, HR, legal/compliance, IT, produzione).

Si concentra su: Privacy, Cyber Security e Business Continuity.

Permette di avere una visione generale della situazione

Fornisce indicazioni sulle attività da svolgere per adeguarsi alle nuove prescrizioni.

MYWAY SECURITY SOLUTIONS

PRIVACY IMPACT ASSESSMENT – PIA
(valutazione di impatto)

E’ una valutazione dei rischi (es. perdita dei dati, furto, uso illecito, etc.) a cui sono sottoposti i dati personali, dei possibili impatti e delle misure di sicurezza, organizzative e tecniche, adottate dall’azienda per il loro trattamento.

E’ una nuova attività prevista dal Regolamento

Fornisce indicazioni sul profilo attuale di rischio dell’azienda in relazione al trattamento dei dati

Permette di identificare gli adempimenti e le attività per risolvere le cr

VULNERABILITY ASSESSMENT

Vengono utilizzati tool automatici che svolgono una lunga serie di controlli su ogni singolo sistema, applicazione o sito e permettono di conoscere dettagli riguardanti la loro configurazione e l'eventuale presenza di vulnerabilità.

Permette di avere una fotografia dello stato di esposizione dei propri sistemi a tutte le vulnerabilità note.

PENETRATION TEST

Simula delle vere e proprie intrusioni, ipotizzando diversi scenari di attacco e combinando tecniche manuali all'utilizzo degli strumenti automatici.

Permette di analizzare l'esposizione a vulnerabilità meno evidenti e, soprattutto, di mostrare come lo sfruttamento combinato di vulnerabilità di vulnerabilità singolarmente non possa invece esporre a conseguenze di notevole impatto.

I risultati delle due attività precedenti consentono di pianificare e programmare tutte le azioni da intraprendere per eliminare le criticità emerse.

MYWAY SECURITY SOLUTIONS

BUSINESS IMPACT ANALYSIS - BIA

E’ un’analisi dei rischi per la continuità operativa dei processi operativi più critici per l’organizzazione e degli effetti economici, sul personale, reputazionali e legali/amministrativi che un’interruzione improvvisa delle attività produttive potrebbe causare.

Permette di definire una strategia di ripristino che sarà poi resa attuabile con un piano di continuità operativa.

VERIFICA DISASTER RECOVERY PLAN IT

Permette di verificare l’efficacia delle misure tecnologiche e logistico/organizzative che l’organizzazione ha predisposto per ripristinare i propri sistemi informativi, i dati e infrastrutture necessarie all'erogazione dei processi e dei servizi aziendali, a fronte di gravi emergenze che ne intacchino la regolare attività.

Permette di verificare le procedure di ripristino dei sistemi informativi sono adeguate alle esigenze operative e di compliance dell’azienda

I risultati delle due attività precedenti consentono definire il livello di rischio operativo dell’azienda e le possibile strategie per la continuità operativa (fisica e logica).

ADEMPIMENTI LEGALI E ORGANIZZATIVI

richiesti dal nuovo Regolamento UE sulla protezione dei dati (entro il 25 maggio 2018).

VALUTAZIONE DI IMPATTO SULLA PRIVACY

PRIVACY IMPACT ASSESSMENT - PIA

I nostri esperti in Privacy Impact Assessment produrranno la valutazione dei rischi richiesta dal Regolamento Europeo 679/16

Sostituisce la notificazione. È la **valutazione preliminare dei rischi e degli impatti** a cui andrebbe incontro un processo qualora dovessero essere violate le misure di protezione dei dati. Prevede attività come la mappatura dei dati e dei trattamenti, la pianificazione degli interventi tecnologici e organizzativi di protezione dei dati ed una valutazione complessiva di riduzione dello stato di rischio.

MYWAY SECURITY SOLUTIONS

DATA PROTECTION OFFICER – DPO

(responsabile protezione dati)

E‘ una nuova figura di vigilanza, nominata dal Titolare e dal Responsabile del trattamento. Agisce in modo indipendente ed ha il compito di informare e consigliare l’azienda, di sorvegliare i processi di trattamento, di valutare i rischi per il trattamento e la valutazione d’impatto (PIA), di fungere da contatto con gli interessati e di collaborare con l’Autorità di controllo. Può essere interno o esterno all’azienda.

E’ obbligatorio per le PA e gli organismi pubblici, per alcuni altri soggetti (big data, dati particolari, profilazione) ma è consigliato per tutte le altre aziende.

Data Protection Officer (certificati a livello europeo) per svolgere la funzione di DPO **esterni** presso l’azienda.

AGGIORNAMENTO E IL MIGLIORAMENTO DELLA SICUREZZA LOGICA E FISICA

dei sistemi informativi aziendali

DATA PROTECTION BY DESIGN

fin dall'ideazione e progettazione di un trattamento o di un sistema, dovranno essere applicate **misure tecniche** (es. cifratura, pseudonimizzazione) ed **organizzative** adeguate a tutelare i diritti degli interessati e a gestire possibili problematiche.

DATA PROTECTION BY DEFAULT

per impostazione **predefinita** le organizzazioni dovranno trattare **solo i dati personali necessari** per le finalità previste e solo **per il periodo strettamente necessario**.

I nostri specialisti assisteranno i responsabili aziendali nell'implementazione di misure tecniche per la protezione dei dati

MYWAY SECURITY SOLUTIONS

FORMAZIONE DEI RESPONSABILI E DEI DIPENDENTI

sicurezza logica, information security policy, business continuity

FORMAZIONE IN AZIENDA E AFFIANCAMENTO

PIATTAFORMA DI E-LEARNING

CORSO SULLA SICUREZZA LOGICA: per tutti quelli che utilizzano strumenti informatici. Serve a informare e formare sui rischi e sui comportamenti che espongono l'azienda a possibili sottrazioni di dati.
Aiuta a disincentivare comportamenti e azioni che possono creare, indirettamente, gravi danni all'azienda.

CORSO SULLE POLICY AZIENDALI: per i dipendenti che utilizzano mezzi e strumenti aziendali (autovettura, PC, telefono, cellulare, carta di credito aziendale). Illustra le disposizioni aziendali e le normative vigenti, per rendere più chiari i comportamenti più consoni e corretti da adottare.

CORSO SULLA BUSINESS CONTINUITY: per i responsabili delle varie funzioni aziendali. Introduce i concetti di risk management resilienza aziendale e continuità operativa e forma i manager a progettare la continuità dell'azienda e a gestire la reazione in caso di eventi critici.

La distrazione, l'errore umano o il non tener conto di alcuni accorgimenti, da parte di tutti coloro che utilizzano strumenti informatici aziendali, sono fattori che favoriscono gli attacchi esterni: ed aumentano i rischi per la sicurezza dei dati personali e aziendali.

BUSINESS CONTINUITY PLAN - BCP

Redazione di business continuity plan per permettere all'azienda di riprendere le proprie attività in tempi brevi in caso di eventi critici (es. incendio, terremoto, epidemia, etc.) che dovessero colpirla.

DISASTER RECOVERY PLAN E/O BACK PLAN IT

Predisposizione di un Piano di Disaster Recovery IT e di una procedura di backup dei dati efficaci

Supporto per le certificazioni **ISO 27001** (information security) e **ISO 22301** (business continuity).

Tutte le attività di analisi e di miglioramento dei sistemi e dei processi saranno progettate per essere **già in linea con i requisiti delle norme** e per facilitare la creazione e la certificazione dei sistemi di gestione corrispondenti.

TRASFERIMENTO DEI RISCHI RESIDUI
al mercato assicurativo grazie al KNOW HOW di ASSITECA

POLIZZE CYBER (danni

First Party
forensic e costi di comunicazione; asset data loss; ripristino sistemi; perdite per interruzione esercizio

Third Party Liability
responsabilità civile professionale per sicurezza del sistema e privacy

Garanzia Crime
frodi informatiche e furto di valori e titoli

POLIZZE Property
(danni materiali ai beni)

DANNI al SISTEMA INFORMATICO

BUSINESS INTERRUPTION
(danni per sospensione o interruzione attività)

SPESE LEGALI
(D&O e Assistenza Legale)

Le attività svolte per migliorare la "resilienza" dell'azienda in materia di Privacy, di information security e di business continuity permetteranno ad Assiteca di trasferire con efficacia (costi e coperture) i rischi residui alle Assicurazioni e di ottimizzare il piano assicurativo dell'azienda.

MYWAY SECURITY SOLUTIONS

MONITORAGGIO E MANTENIMENTO

Audit periodici

Consulenza

Assistenza tecnica e specialistica

Personale dedicato

Formazione

E ogni altro supporto richiesto per mantenere o migliorare la resilienza aziendale in materia di Privacy, cyber security, continuità operativa e coperture assicurative.

MYWAY SECURITY SOLUTIONS

GRAZIE

Guido Mondelli
Amministratore Delegato My Way S.r.l.
guido.mondelli@mywaysec.com
335 8050928

Federico Cattabiani
Responsabile Commerciale My Way S.r.l.
f
ederico.cattabiani@mywaysec.com
333 8799083