PRIVACY

che cos'è e perché esiste?

Le norme sulla privacy mirano a tutelare, da un lato, i diritti di persone e società relativamente ai dati che le riguardano; dall'altro sono un punto di riferimento per proteggere le aziende dai pericoli che minacciano il loro patrimonio informativo.

La normativa in materia di privacy disciplina il trattamento di dati personali. Riguarda un numero sempre crescente di ambiti nei quali sono trattate informazioni delicate:
videosorveglianza, gestione dei documenti elettronici,
dati di natura clinica, telemarketing e indagini di mercato, fidelizzazione e profilazione di consumatori, informazioni e assicurazione del credito, dati trattati nel rapporto di lavoro, controllo del traffico internet in azienda.

Orion Informatica
43011 Busseto (PR) - Via Beethoven, 1 Tel. 0524 930119 Fax 0524 680209 Cell. 348 5421264
www.orion-informatica.com

cosa dice la legge?

La legge prevede che le aziende prendano in considerazione i rischi esistenti per i propri dati; si tratta di una forma di tutela sanzionata in ambito sia penale sia amministrativo.

perché adeguarsi ?

Il codice privacy è pienamente vigente e le sue violazioni sono sanzionate dalle autorità competenti.

- In caso di **violazione** accertata, sono previste **sanzioni** di tipo amministrativo (multe fino a 124.000 Euro) e la reclusione (fino a 3 anni), **esclusione dalle gare di appalto**, risarcimenti danni. L'Autorità Garante effettua ispeziona e sanziona gli inadempienti insieme alla Guardia di Finanza.
- Opportuno valutare, oltre alle sanzioni e alle perdite economiche, anche i **danni all'immagine**.
- Il rapporto tra rischio di perdita e costo dell'adeguamento è **inferiore al 2**%.
- In ambito pubblico l'avanzare del governo elettronico pone molteplici problematiche da risolvere in materia di tutela dei dati personali. **La tutela della privacy rientra nei progetti qualità e negli accreditamenti istituzionali.**
- Le risorse immateriali (le informazioni in generale) sono destinate a diventare sempre più importanti. La legge sulla privacy, considerato il vertiginoso sviluppo delle nuove tecnologie, è destinata a rivestire un ruolo fondamentale.

come si adeguano le aziende

Adeguarsi alla normativa e ai suoi requisiti richiede di considerare sia gli aspetti tecnologici che quelli organizzativi: la gestione sicura del proprio patrimonio informativo significa prendere coscienza dei rischi esistenti e prevedere delle contromisure.
Per adeguarsi, l'azienda, è tenuta ai seguenti comportamenti:
contromisure tecnologiche, garantire la sicurezza dei sistemi informatici richiede di intervenire sulle tecnologie utilizzate; in diversi casi è sufficiente configurare in modo adeguato ciò di cui si dispone già.

Contromisure organizzative. Si tratta di definire ruoli, responsabilità e incarichi in relazione ai trattamenti.

Adempimenti di carattere formale. Sono previste alcune comunicazioni formali, generalmente verso i soggetti a cui appartengono i dati trattati (clienti, fornitori, dipendenti); in alcuni casi sono richieste comunicazioni verso il Garante.

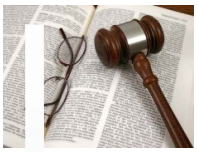
sanzioni

Sanzioni amministrative	
Omessa o inidonea informativa	Da € 3.000,00a € 18.000,00
Omessa o inidonea informativa (dati sensibili, giudiziari o che presentano rischi specifici)	Da € 5.000,00 a € 30.000,00
Cessione illecita di dati	Da € 5.000,00 a € 30.000,00
Violazioni dei dati idonei a rivelare lo stato di salute	Da € 500,00 a € 3.000,00
Omessa o incompleta notificazione	Da € 3.000,00 a € 18.000,00
Omessa informazione o esibizione al Garante	Da € 3.000,00 a € 18.000,00

Illeciti penali	
Trattamento illecito di dati	Reclusione da 6 a 24 mesi
Trattamento illecito di dati (dati sensibili, giudiziari o che presentano rischi specifici)	Reclusione da 1 a 3 anni
Falsità nelle dichiarazioni e notificazioni al Garante	Reclusione da 6 mesi a 3 anni
Omessa adozione delle misure minime di sicurezza	Arresto fino a 2 anni o la sanzione pecuniaria da € 10.000,00 a € 50.000,00
Trattamento dei dati in violazione delle misure di sicurezza	Arresto fino a 2 anni e la sanzione amministrativa da € 20.000,00 a € 120.000,00

altri rischi

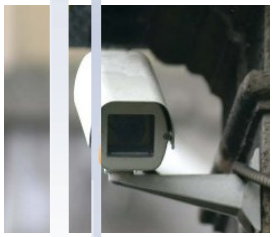
Inoltre l'azienda deve tener conto anche di altri rischi:



Responsabilità civile. Il Codice prevede, a carico delle aziende, anche una responsabilità civile in caso di danni derivati da un trattamento non conforme dei dati, oppure dalla mancata applicazione delle misure di sicurezza. Questo significa che l'azienda potrebbe dover pagare un risarcimento a chi ha subito il danno (ad esempio per la diffusione non autorizzata di informazioni su un cliente dalle quali sia derivato un danno a quest'ultimo).

Danno alla propria immagine. Un'azienda che non tratta i dati in modo corretto e trasparente rischia di perdere in credibilità, fiducia e professionalità.
In particolare, essere vittima di un attacco informatico o un incidente di sicurezza fornisce all'esterno un'immagine estremamente negativa e poco affidabile.

Esposizione del patrimonio informativo aziendale. Si tratta del rischio più grave, ma anche del più sottovalutato. Le informazioni di un'organizzazione sono il suo patrimonio più importante. Trascurare la sicurezza delle informazioni significa mettere a rischio il proprio business e il valore stesso dell'azienda.



come avvengono i controlli

L'autorità competente, il Garante per la Privacy, effettua i controlli impiegando un nucleo specializzato della Guardia di Finanza.

Le verifiche sul rispetto della normativa possono essere condotte:

- a seguito di una segnalazione o a una denuncia;
- in base al piano ispettivo approvato annualmente dal Garante per la Privacy;
- come conseguenza di un altro tipo di controllo (ad es. fiscale).

IL NOSTRO RUOLO

adeguarsi significa benefici per il business

Un' azienda che adotta politiche di sicurezza delle informazioni si propone sul mercato come un partner **affidabile e sicuro.**

Sul piano organizzativo gli interventi si integrano con i sistemi per la qualità adottati da molte aziende.

Adeguarsi non significa solo rispondere a un obbligo di legge, ma permette di garantire la protezione dei propri valori e del proprio patrimonio aziendale più importante, quello informativo.

il nostro approccio in azienda

Un approccio attivo e cosciente alla Normativa Privacy fa si che si posizioni come un valore aggiunto per economia.

Non più come un ostacolo, ma un ausilio, che i soggetti economici possono utilizzare per affermare un modello in cui la competizione nel mercato e la conquista del cliente e dei risultati siano compatibili con il rispetto della persona.

adeguamento al codice

Attraverso i punti elencati di seguito si intendono realizzare i documenti e le procedure necessarie all' adeguamento al Codice in materia di protezione dei dati personali ed identificare le linee guida che, nel rispetto della normativa, permettano di operare nell'ottica di tutela degli interessi aziendali.

analisi strutturale aziendale

E' l'insieme delle attività che permettono di definire quale corretta strategia di adeguamento adottare e attraverso quali strumenti.
Prevede la raccolta e lo studio delle informazioni concernenti la struttura operativa e funzionale dell'azienda, in particolare:

- Mappatura dei trattamenti dei dati
- Tipologia dati trattati, modalità di raccolta e di trattamento
- Incaricati ai vari trattamenti e categorie di interessati
- Terzi soggetti preposti al trattamento (outsourcer)
- Definizione dell'organizzazione aziendale
- Organigramma aziendale funzionale rispetto ai trattamenti dati, con evidenza degli eventuali responsabili e incaricati
- Processi aziendali interessati al trattamento
- Amministratori di Sistema
- Mappatura del Sistema informativo
- Edifici e locali dove avvengono i trattamenti
- Strumenti informatici, di telecomunicazione e di sicurezza
- Archivi fisici, archivi elettronici, software utilizzati
- Misure di sicurezza vigenti

realizzazione documentale

Al termine delle attività di analisi, viene redatta la documentazione necessaria a soddisfare l'adeguamento alla normativa e l'implementazione della strategia scelta, in particolare:

- Nomine di responsabili interni e in outsourcing
- Individuazione incaricati
- Informative ed eventuali consensi per categoria di interessati
- Eventuali autorizzazioni e notificazioni
- Procedure operative in materia di privacy e misure minime di sicurezza
- Linee Guida sull'utilizzo degli strumenti informatici, internet e mail
- Documento sulle misure di sicurezza adottate per la struttura IT.

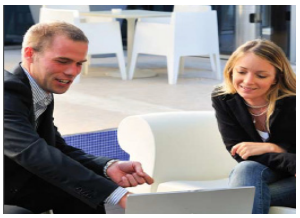
amministratori di sistema

Prevede l'adeguamento al provvedimento specifico, attraverso:

- Nomina amministratori di sistema
- Creazione credenziali coerenti con le autorizzazioni previste dalle nomine
- Soluzione raccolta log di accesso

formazione incaricati

La collaborazione degli incaricati è fondamentale per prevenire eventi dannosi e il momento della formazione è cardine per coinvolgerli in termini di responsabilità e consapevolezza. Le misure tecniche non sono da sole sufficienti a proteggere i dati: il comportamento corretto di chi tratta i dati, oltre a costituire un obbligo di legge, è fattore indispensabile per una efficace attuazione della sicurezza.
La formazione fornisce le nozioni di base sul codice in materia di protezione dei dati personali. Prevede la spiegazione dei regolamenti e delle linee guida adottate.



analisi responsabili

Oltre alla formazione sopra descritta, per i responsabili è possibile prevedere una sessione supplementare per approfondire la tematica relativa ai Regolamenti sull'utilizzo dei sistemi informatici e telefonici, alla proprietà aziendale delle caselle di posta elettronica, alla videosorveglianza alle procedure permesse riguardo le modalità di verifica e controllo del personale.

documentazione e verifica misure di sicurezza informatiche

Occorre che il sistema informativo sia adeguato alle direttive ed ai regolamenti approvati.
La documentazione comprenderà le linee guida per ottenere un efficiente sistema di sicurezza:

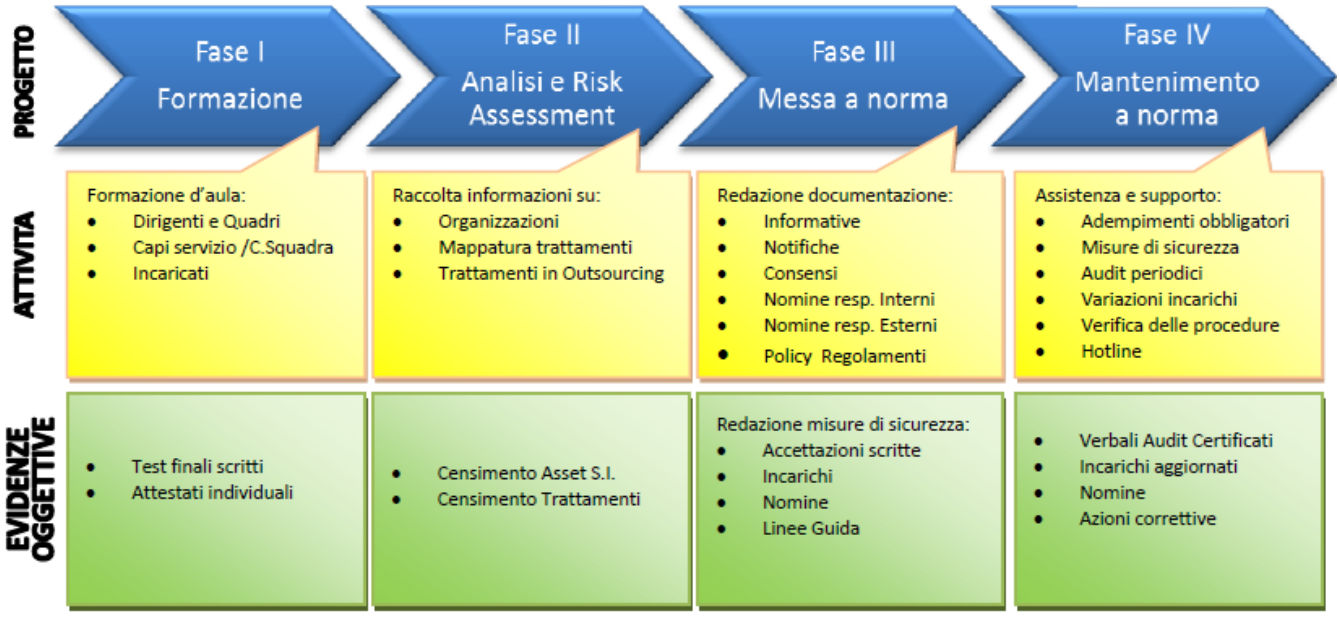
- mappatura dei criteri di accesso alla rete
- gestione backup e sviluppo di un piano di Disaster Recovery
- gestione della rete e controllo degli accessi non autorizzati
- gestione credenziali e tipologie di autenticazione
- regolamentazione della navigazione su internet
- regolamentazione dell'utilizzo delle mail aziendali
- analisi delle soluzioni di cloud computing
- regolamentazione delle condivisioni di rete per ottimizzare i processi
- pianificazione dei controlli da effettuare sulle aree più a rischio
- regolamentare l'utilizzo di dispositivi mobili (tablet, smartphone, notebook…)
- linee guida per la gestione degli incidenti sulla struttura informatica
- relazione sui possibili miglioramenti ICT

L' analisi della rete informatica verrà effettuata sui seguenti punti:

- verifica installazione e aggiornamento di apparecchiature firewall
- verifica adozione di un sistema di back-up
- pianificazione della procedura per la custodia delle copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- verifica adozione di un sistema di stabilizzazione di corrente
- verifica, codifica e separazione dati sensibili se tenuti in banche dati
- verifica dell'integrità del sistema operativo
- verifica installazione e aggiornamento di software antivirus e di protezione
- verifica cifratura o separazione dati sensibili
- definizione scritta di procedure per l'assegnazione dei codici di autenticazione informatica agli utenti a seconda della loro nomina e del gruppo di appartenenza e per l'archiviazione dei dati
- assegnazione ad ogni utente degli elaboratori di Username e password
- nomina dei gestori della manutenzione degli strumenti elettronici, pianificazione di interventi periodici per il corretto funzionamento degli elaboratori
- verifica di congruità di eventuali software o sistemi di controllo già in uso
- verifica di protezione di eventuali reti wi-fi

In caso di riscontro di irregolarità nelle apparecchiature o nei software, provvederemo ad indicarvi le modifiche necessarie da applicare.

LE FASI DEL PROGETTO



PRINCIPALI VANTAGGI NELL'ATTUAZIONE DELLA MESSA A NORMA SECONDO IL D. LGS. 196/03 SULLA PRIVACY.

- **Deresponsabilizzazione** della società e dell'Amministratore (nei confronti di un errato o doloso comportamento di un dipendente o di un agente).
- Controllo e tutela del **patrimonio aziendale.**
- **Tutela** del portfolio clienti della società (contro un utilizzo improprio da parte degli agenti).
- Migliore gestione delle **azioni di marketing.**
- Corretto **controllo** dell'operato dei propri dipendenti sulle loro attività informatiche.
- **Tutela** delle informazioni aziendali (contabili, amministrative, vendita).
- Corretta definizione di **compiti/responsabilità.**
- Verifica dell'attuale **sicurezza** e struttura della rete informatica.
- Verifica **responsabilità** dell'amministrazione della rete informatica.

mantenimento a norma

Per gli anni successivi a quello di messa a norma, offriamo un servizio di mantenimento attraverso il quale garantiamo la continuità nell'applicazione della normativa e lo sviluppo delle linee guida e dei regolamenti concordati durante l'analisi.
Abbiamo configurato tre livelli di prestazione, che comprendono:

ABBONAMENTO ANNUALE "***Audit***" – scade il 31/12 di ogni anno
Prevede una visita annuale presso la vostra sede per:

- *verifica trattamenti e relative procedure;*
- *verifica moduli informativa e consenso, verifica incarichi per il personale addetto;*
- *eventuale aggiornamento, istruzioni e procedure per gli incaricati;*
- *aggiornamento incarichi in outsourcing per i gestori esterni dei vostri dati;*
- *redazione Manuale Organizzativo Privacy;*
- *eventuale aggiornamento linee guida utilizzo internet, mail aziendale e attrezzature elettroniche ed informatiche;*
- *verifica norme minime di sicurezza e relativa verbalizzazione come da Allegato B;*
- *verifica operato Amministratori di Sistema (se presenti);*
- *servizio telefonico per qualsiasi necessità privacy relativa a incaricati e interessati.*

Il servizio prevede l'invio di regolari comunicazioni riguardo l'aggiornamento della normativa e la modifica degli incarichi interni ed esterni su richiesta del cliente.
Il servizio non include le prestazioni specificate negli abbonamenti "Protect" e "Defend"

ABBONAMENTO ANNUALE "Protect" – scade il 31/12 di ogni anno
Include le prestazioni dell'abbonamento "***Audit***" con, in aggiunta:

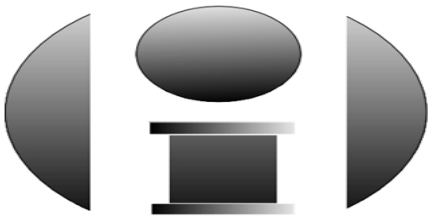
- due visite annuali anziché una;
- valutazione sicurezza della struttura informatica;
- in caso di emanazione di nuovi provvedimento da parte dell'Autorità Garante o di
- aggiornamenti della normativa vigente, si provvederà a regolarizzare la struttura.

ABBONAMENTO ANNUALE "Defend" – scade il 31/12 di ogni anno
Include le prestazioni dell'abbonamento "***Protect***" con, in aggiunta:

- consulenza via mail annua senza limiti di invio, compresi pareri legali;
- studio e redazione riscontri di accesso pervenuti alle strutture da soggetti terzi.
- redazione dell'eventuale corrispondenza della fase stragiudiziale in caso di contenzioso

Si intendono sempre esclusi e soggetti a valutazione separata:

- la richiesta di ulteriori interventi formativi
- la regolarizzazione di nuovi trattamenti iniziati dopo il primo adeguamento



Orion Informatica
43011 Busseto (PR) - Via Beethoven, 1
Tel. 0524 930119 Fax 0524 680209
Cell. 348 5421264

www.orion-informatica.com

in collaborazione con:

polaris

43036 FIDENZA (PR)
VIA XXIV Maggio 28/C
www.polaris.it