

Privacy ... in pratica



Guida semplice per capire la normativa per la protezione e tutela dei dati personali

Decreto Legislativo n. 196 del 30 Giugno 2003

Cosa ci ha spinto

Caro Lettore,

spesso per ragioni professionali o per pura sete di conoscenza desidereremmo avere tutto a portata di mano. Ancora spesso ci lamentiamo della "durezza" con le quali vengono scritte le norme e questo susseguirsi fa scaturire in noi una certa apatia (o antipatia) per la legge in genere. Certo se c'è interesse fervido per la materia in questione la passione ci spinge ad essere divoratori non solo della fonte (normativa, appunto) ma anche di tutti i commenti, insomma, anche delle più piccole informazioni.

Ma quando non siamo presi da questa passione verso una determinata materia? E quando, a prescindere dalla passione, dobbiamo conoscere quella materia per ragioni di lavoro?

Vi e' mai capitato di desiderare un prontuario, un riassunto, una tabella o documento pratico di facile comprensione che vi permetta di conoscere una materia per quanto vi occorra?

Certo che si ... anche noi desideriamo avere, subito, informazioni!

Da qui la nostra idea di preparare un documento "a taglio pratico" per "far capire" la normativa della privacy anche a coloro che ne sono completamente a digiuno.

E questo nostro impegno è utile per:

- gli operatori economici e professionali, nel chiaro intento di "informarsi" su quanto detta il codice della privacy
- tutti i soggetti che desiderano avere una base di partenza da approfondire successivamente con letture "più dottrinali"
- per tutti coloro che hanno bisogno di una piccola rinfrescata sul loro sapere

Ringraziandoti per la fiducia riposta in noi, ti preghiamo, con lo spirito di rendere sempre migliore la qualità dei nostri servizi, di proporci suggerimenti o di scriverci le tue considerazioni siano esse positive che negative a:

"La saggezza si acquisisce dalle esperienze e, generalmente, le esperienze negative sono frutto degli errori !!!"

... le origini della normativa

Le norme antecedenti

- √ Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
- √ D.p.r. 28 luglio 1999 n. 318 - Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, c. 2, della legge 31 dicembre 1996, n. 675
- √ Legge 3 novembre 2000 n. 325 - Disposizioni inerenti l'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'articolo 15 della L. 31/12/96, n. 675.

La Legge 675/96: il punto di partenza della privacy

La legge 675/96 sulla tutela dei dati personali (legge sulla privacy), ed i successivi decreti attuativi, hanno imposto alle aziende una serie di obblighi mirati a tutelare la privacy dei propri dipendenti, dei clienti, dei fornitori ed in generale di tutti i soggetti di cui l'azienda detiene dati personali o "particolari" (dati sensibili e dati giudiziari).

E' un testo unico ... questo in vigore!

Il testo unico in materia di protezione dei dati personali, è stato definitivamente approvato dal Consiglio dei ministri il 27 giugno 2003 e denominato "Codice della Privacy", dove sono state identificate maggiori garanzie per i cittadini, migliorato e semplificato le norme esistenti. Il provvedimento, racchiude in un solo testo la normativa vigente e gli altri decreti legislativi, regolamenti e codici deontologici succeduti in questi anni, e sono presenti anche integrazioni importanti per quanto riguarda le comunicazioni elettroniche.

Quindi il nuovo Codice, rappresenta il primo tentativo di unificare le disposizioni relative alla privacy in un unico testo normativo ... entrato in vigore il 1° Gennaio 2004.

Introduzione alla Privacy

Privacy: derivazione del termine

E' un termine inglese che si accosta ai concetti di "riservatezza", "privatezza".

Cosa significa, oggi, la privacy

Oggi, la privacy oltre ad esprimere il diritto di essere lasciati in pace o di proteggere la nostra sfera privata, ci pone nella condizione anche di controllare l'uso e la circolazione dei nostri dati personali. Ci rende liberi di decidere chi può conoscere le nostre informazioni personali.

La privacy e, in particolare, la protezione e tutela dei dati personali costituiscono un diritto fondamentale dell'essere umano, strettamente connesso alla tutela della dignità umana.

Il Garante

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente concepita già dalla vecchia legge privacy n. 675 del 31 dicembre 1996, ed è presente in tutti gli altri Paesi membri dell'Unione Europea. Il compito del Garante è di assicurarci la difesa dei diritti e delle libertà fondamentali nel trattamento dei dati personali ed il rispetto della dignità della persona.

Segnalazioni e ricorsi

Il Garante provvede all'accertamento delle segnalazioni da parte dei cittadini e vigila affinché tutte le norme previste per la tutela della vita privata di ogni singolo interessato, vengano rispettate. Ha potere decisionale sui ricorsi presentati e può impartire ispezioni di controllo.

Per cosa si impegna il Garante?

Come già detto, il Garante può ricevere segnalazioni e ricorsi dai cittadini, compiere ispezioni di controllo, procedere con sanzioni amministrative pecuniarie in caso di violazione della normativa, in questo caso viene informata l'autorità giudiziaria, la quale provvederà ad effettuare eventuali sanzioni.

E ... a cosa serve il Garante?

Ha l'autorità di bloccare trattamenti di dati che possono arrecare danno agli interessati, accertandosi della sicurezza degli stessi, garantendo così il rispetto della dignità dell'interessato, con importante riferimento alla riservatezza delle persone.

Dato Personale: Definizione ...

"Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

Quindi qualsiasi informazione toccante la sfera intima e personale di terzi riguardo a persone, società, enti, associazioni identificati o identificabili attraverso altre informazioni, ad esempio, un numero o un codice identificativo.

Si considerano, quindi, dati personali:

- √ nome e cognome o denominazione;
- √ indirizzo o sede;
- √ codice fiscale, partita iva, numero iscrizione registro imprese, etc;
- √ una foto, un video, la registrazione della voce;
- √ una impronta digitale
- √ ...

La persona può essere riconosciuta e identificata anche attraverso altre notizie: ad esempio, associando la registrazione della voce di una persona alla sua immagine, oppure alle circostanze in cui la registrazione è stata effettuata: luogo, ora, situazione.

Trattamento di Dati Personali: definizione ...

"Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".

Pertanto il trattamento è un'operazione o complesso di operazioni che vengono effettuati per la gestione dei dati personali.

Su quali trattamenti di dati personali si applica la legge?

La legge non si applica ai trattamenti "per fini esclusivamente personali" come la gestione della propria agenda elettronica o cartacea, oppure una rubrica, o la propria posta personale.

Vi sono poi altri trattamenti (ad esempio, quelli effettuati dal Centro elaborazione dati del Dipartimento di pubblica sicurezza, oppure dai servizi di sicurezza, o dal casellario giudiziale, o dagli uffici giudiziari per ragioni di giustizia o quelli effettuati per scopi di difesa o sicurezza dello Stato ovvero per il perseguimento di reati) che sono soggetti solo in parte all'applicazione delle disposizioni della legge sulla privacy.

La legge si applica anche agli archivi o alle banche dati?

Certo, la legge si applica ad ogni operazione di trattamento di dati relativi alle persone a prescindere dall'esistenza di archivi o banche dati.

E se tratto i dati soltanto con moduli cartacei?

Comprendete bene, la legge si applica a tutti i trattamenti indipendentemente dal fatto che siano realizzati "con l'ausilio di strumentazioni elettroniche (Computer), o che avvenga con sistemi diversi da strumentazioni elettroniche (apparecchiature video, moduli cartacei).

Chi è l'Interessato ...

"La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali".

Pertanto e' definito soggetto "interessato" la persona, l'impresa, l'associazione, l'ente pubblico ecc. cui si riferiscono i dati personali (quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale ecc. di LUIGI BIANCHI o della BRIXIA BUSINESS SOLUTIONS, LUIGI BIANCHI e la BRIXIA BUSINESS SOLUTIONS sono rispettivamente gli "interessati").

Quali sono i diritti in favore dell'interessato ?

La legge sulla privacy riconosce e garantisce all'interessato una serie di diritti per quanto riguarda il trattamento dei dati personali. In sintesi:

- a) il diritto di avere informazioni generali sui trattamenti di dati svolti nel nostro Paese (attraverso la consultazione gratuita del registro dei trattamenti)
- b) il diritto di accesso ai propri dati personali direttamente presso chi li detiene (titolare del trattamento) - ossia il diritto di ottenere la conferma della loro esistenza e la loro comunicazione e di sapere da dove sono stati acquisiti e quali sono i criteri e gli scopi del trattamento, in questo caso il titolare può chiedere il pagamento di una somma ("contributo spese") se non detiene dati dell'interessato
- c) il diritto di ottenere la cancellazione o il blocco di dati che sono trattati violando la legge (ad esempio, perché non è stato chiesto il consenso); tali diritti possono essere esercitati anche quando non ci sono più motivi validi per conservare i dati
- d) il diritto di aggiornare, correggere o integrare i dati inesatti e incompleti
- e) il diritto, nei casi indicati nelle lettere c) e d), di ottenere anche un'attestazione da parte del titolare che tali operazioni sono state portate a conoscenza dei soggetti ai quali i dati erano stati precedentemente comunicati - a meno che ciò risulti impossibile o richieda un impegno sproporzionato rispetto al diritto tutelato
- f) il diritto di opporsi, per motivi legittimi, al trattamento dei propri dati
- g) il diritto di opporsi al trattamento dei propri dati per scopi di informazione commerciale o per l'invio di materiale pubblicitario o di vendita diretta, oppure per ricerche di mercato.

Il consenso! Ma cos'è?

Il consenso è la libera manifestazione dell'interessato con cui questi accetta consapevolmente, liberamente ed espressamente un determinato trattamento dei suoi dati personali, sul quale è stato preventivamente informato da chi ha richiesto e gestirà i suoi dati.

Pertanto, non è assolutamente possibile trattare dati personali senza il consenso dell'interessato che, prima ancora, deve essere informato ai sensi dell'art. 13 del Codice: e questa è una regola generale che subisce deroghe in taluni casi.

Per i dati non sensibili? Necessario sempre il consenso?

Certo che no, in alcuni casi il trattamento può essere effettuato anche senza consenso degli interessati. In particolare, può avvenire senza il consenso degli interessati se:

- √ i dati sono stati raccolti e sono conservati perché così prescrive la legge o un regolamento o una norma comunitaria
- √ il trattamento di dati è necessario per adempiere agli obblighi previsti da un contratto
- √ i dati sono ricavati da pubblici registri, atti o documenti che chiunque può conoscere
- √ il trattamento ha scopi scientifici o statistici e rispetta il relativo codice di deontologia
- √ il trattamento è effettuato per scopi giornalistici (si applica anche il codice deontologico per i giornalisti)
- √ i dati riguardano lo svolgimento di attività economiche (ad esempio, i dati relativi al fatturato di un'azienda), e non si violano eventuali segreti aziendali o industriali
- √ occorre salvaguardare l'incolumità fisica o la vita dell'interessato (o di un terzo) che non è in grado di dare il consenso (è il caso dei trattamenti sanitari d'urgenza)
- √ il trattamento è necessario per far valere o a difendere un diritto in sede giudiziaria (ad esempio, per l'istruzione di un processo, per la preparazione del dibattimento ecc.)

I soggetti pubblici ... anche loro debbono richiedere il consenso per il trattamento dei dati non sensibili?

I soggetti pubblici (pubblica amministrazione, enti locali, alcuni enti previdenziali e assistenziali, regioni, etc.) non hanno l'obbligo di richiedere nessun consenso da parte degli interessati, poiché la legge consente loro di effettuare trattamenti di dati personali soltanto per lo svolgimento delle funzioni istituzionali, nei limiti pre-stabiliti dalle leggi e dai regolamenti.

Cos' è un Dato Sensibile?

"I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".

Quindi in parole semplici un dato personale sensibile, per la sua delicatezza, richiede particolari cautele.

Riguardano la razza, l'appartenenza etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti o sindacati, lo stato di salute e la vita sessuale delle persone.

Quali precauzioni vanno adottate per la gestione dei dati sensibili?

I soggetti privati possono far uso di questa tipologia di dati solo in base alle autorizzazioni del Garante e al consenso volontario e scritto da parte degli interessati.

I soggetti pubblici, invece, non devono richiedere il consenso, solo per svolgere determinati trattamenti per interesse pubblico, che dovranno essere disciplinati dettagliatamente con propri regolamenti.

Per il trattamento dei dati sullo stato di salute in ambito sanitario pubblico e privato, esiste una particolare disciplina secondo la quale tale trattamento può essere svolto, di regola, soltanto con il consenso dell'interessato, se ciò serve per tutelare la sua salute o l'incolumità fisica. Per alcune specifiche esigenze di tutela della salute di terzi o della collettività (prevenzione e cure di malattie, ricerca medica ed epidemiologica, interventi in materia di igiene e sanità pubblica ecc.) gli "esercenti le professioni sanitarie" e gli organismi sanitari pubblici (ASL, enti ospedalieri, medici-chirurghi) possono trattare i dati sanitari anche senza il consenso dei pazienti interessati, ma nel rispetto delle prescrizioni contenute in un'autorizzazione del Garante (n. 2/2000).

Trattamento di dati sensibili ... con o senza consenso ...

Solo in questi casi il trattamento dei dati sensibili e' possibile senza il consenso dell'interessato:

- √ quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo.
- √ quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo.
- √ quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive.
- √ quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza.

Parliamo di Notificazione al Garante ...

La notificazione è una comunicazione che il titolare del trattamento deve trasmettere una tantum facendo uso di un apposito modulo da inviare al Garante, in cui vengono elencate le principali caratteristiche del trattamento (categorie dei dati trattati, finalità del trattamento, luogo ove avviene il trattamento, soggetti, in Italia o all'estero, ai quali i dati sono eventualmente comunicati, misure di sicurezza adottate).

La Notificazione va inviata prima che il trattamento abbia inizio, e non va ripetuta, a meno che non vi siano modifiche delle caratteristiche di trattamento (quindi, se per esempio cambiano le finalità del trattamento o cambia la ragione sociale del titolare, la notificazione deve essere nuovamente presentata al Garante).

Tutte le notificazioni pervenute al Garante sono riposte in un "registro dei trattamenti" accessibile al pubblico.

La stragrande parte dei Titolari, però, non è soggetta a questa fase di notificazione in quanto il Garante ha emanato un apposito provvedimento in materia.

Una cosa deve essere tenuta ben in mente: la notificazione consiste solo nella descrizione degli archivi e delle banche dati, e non nella trasmissione del loro contenuto (ossia di tutti i dati personali in possesso del titolare).

Quando si può fare a meno di presentare la Notificazione?

Come dicevamo prima, la stragrande dei soggetti non è tenuta ad effettuare alcuna azione di notifica ed i casi più frequenti sono quelli in cui:

- √ il trattamento è previsto da norme di legge o di regolamento
- √ riguarda dati non relativi ad individui ma soltanto ad imprese, società, enti o associazioni
- √ esistono dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque (atti anagrafici e dello stato civile, registro delle imprese, liste elettorali)
- √ Il trattamento è finalizzato al rispetto di specifici obblighi contabili (bilanci), retributivi (paghe e stipendi), previdenziali e assistenziali (contributi pensionistici), fiscali (fatture, dichiarazioni dei redditi)
- √ Il trattamento è effettuato da piccoli imprenditori (secondo la definizione del codice civile), da liberi professionisti iscritti in albi o da associazioni, fondazioni, organismi non a scopo di lucro

E' opportuno fare riferimento all'articolo 7 della legge per ricavare un elenco completo dei molti casi di esonero e di dichiarazione semplificata (e delle condizioni previste caso per caso).

***Abbiamo capito chi è l'interessato e cosa sono i dati!
Ora è importante comprendere chi sono
i soggetti che gestiscono queste informazioni***

Titolare del trattamento: definizione e ... in parole semplici

"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza".

La persona, ditta, ente, associazione etc., a cui fa capo effettivamente il trattamento di dati personali e al quale spetta assumersi la responsabilità delle decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza).

Nei casi in cui il trattamento sia effettuato da una società e da una pubblica amministrazione per titolare si intende l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, legale rappresentante pro-tempore, direttore generale ecc.). I casi in cui il trattamento può essere imputabile ad un individuo riguardano semmai liberi professionisti o ditte individuali.

Il Responsabile del trattamento

"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali"

Pertanto la persona, la società, l'ente, l'associazione o l'organismo a cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, incarichi di gestione e controllo del trattamento dei dati.

L'Incaricato del trattamento

"le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".

Quindi il dipendente o il collaboratore che per conto della struttura del titolare elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare medesimo (e/o dal responsabile, se designato).

L'Informativa: cos'è?

L'informativa rappresenta (su fatture, su pagine web, su fax, su mail, a voce, etc.) le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto, quando vengono raccolti dati presso l'interessato stesso, oppure presso terzi. Ovvero:

- √ su quali sono gli scopi (finalità) e le modalità del trattamento
- √ se l'interessato è obbligato o no a fornire i dati
- √ quali sono le conseguenze se i dati non vengono forniti
- √ a chi possono essere comunicati o diffusi i dati raccolti
- √ quali sono i diritti riconosciuti all'interessato
- √ chi sono il titolare e il responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax ecc.)

Quando rendere l'Informativa?

Sempre, a meno che:

- √ le informazioni siano già state fornite all'interessato
- √ le informazioni possano ostacolare attività di ispezione o controllo
- √ per la prevenzione o la repressione dei reati
- √ i dati non siano stati raccolti presso l'interessato, sia impossibile fornire l'informativa o comunque tale adempimento comporti un impiego
- √ di mezzi giudicato dal Garante "manifestamente sproporzionato"
- √ il trattamento sia previsto da norme di legge o di regolamento
- √ sia necessario per la difesa dei propri diritti in sede giudiziaria

Si consiglia, vivamente, di comunicare l'informativa ad ogni singolo interessato (dipendenti e collaboratori, clienti, fornitori, professionisti, ecc.) anche se la normativa non ne prevede l'obbligo per taluni casi.

Questo perchè, viste le sanzioni pesanti del Codice, la prova dell'avvenuta comunicazione può essere utilizzata in fase giudiziaria in caso di opposizione da parte dell'interessato.

Autorizzazione del Garante: definizione ...

L'autorizzazione è il provvedimento adottato dal Garante attraverso il quale autorizza il titolare del trattamento (ente, azienda, libero professionista) a trattare determinati dati "sensibili" o giudiziari o a trasferire gli stessi all'estero.

In tema di dati sensibili e giudiziari, il Garante ha emanato alcune "autorizzazioni generali" che consentono a varie categorie di titolari di trattare dati per gli scopi specificati senza dover chiedere singolarmente un'apposita autorizzazione al Garante.

Comunicazione: definizione ...

"Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal

responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione”

Mettere uno o più soggetti determinati, che non siano l'interessato, a conoscenza di dati personali tramite qualsiasi mezzo, sia elettronico che non.

Diffusione: definizione ...

“Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione”

Divulgare, rendere noti dati personali al pubblico o ad un numero indeterminato di soggetti (ad es., è diffusione la pubblicazione di dati personali su un giornale o su una pagina internet).

Cosa sono le Misure di Sicurezza?

Sono gli accorgimenti e i dispositivi utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, fare in modo che solo le persone autorizzate possano accedere ai dati e che vengano effettuati solo trattamenti a norma di legge o per le finalità per le quali i dati erano stati raccolti.

Rispetto alle più ampie misure che il titolare deve applicare a tutela dei dati, un regolamento ha indicato le misure di sicurezza che è obbligatorio adottare per garantire un livello minimo di protezione e per non incorrere in sanzioni anche penali.

Nel regolamento sono fissati una serie di criteri e accorgimenti (ad esempio definizione password e variazione, programma antivirus, firewall software o di tipo fisico, copie degli archivi informatici) che i titolari devono adottare a seconda che il trattamento riguardi dati sensibili e sia effettuato manualmente (archivi e documenti cartacei) o con elaboratori (in quest'ultimo caso, distinguendo tra elaboratori accessibili in rete o meno).

E' previsto che tali misure siano adeguate periodicamente.

Il nuovo Codice della Privacy

Un po' di numeri ...

- √ Il codice si compone di 3 parti
- √ Gli articoli di legge sono 186
- √ N. 3 Codici deontologici allegati
- √ N. 1 Disciplinare tecnico allegato
- √ N. 1 tavola di corrispondenza con le norme precedenti

Il Codice è diviso in tre parti

La prima parte è dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato.

La seconda è la parte speciale dedicata a specifici settori: questa sezione, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori.

La terza parte affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

La semplificazione della notificazione

Una delle principali semplificazioni riguarda l'adempimento della notificazione al Garante, ovvero l'atto con cui l'impresa, il professionista o la pubblica amministrazione segnala all'Autorità i trattamenti di dati che si intendono effettuare.

Mentre con la vecchia normativa (legge 675/1996 e le successive modificazioni) dovevano essere notificati tutti i soggetti non esplicitamente esentati, con la nuova normativa (D.Lgs. 196/2003 Testo unico) viene rovesciata tale impostazione, con conseguente indicazione dei soli pochi casi nei quali la notifica va effettuata.

Il Titolare deve notificare al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

- √ dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- √ dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- √ dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- √ dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;

- √ dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- √ dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Si procede alla notifica solo in particolari casi di trattamento di dati sensibili (specie se sanitari) con determinate modalità d'uso, ma anche per trattamenti particolarmente a rischio, effettuati con strumenti elettronici, come per la registrazione dell'utenza ad un sito web, oppure in relazione a procedure di selezione del personale e ricerche di marketing, nonché in ipotesi di utilizzo di informazioni commerciali e relative alla solvibilità.

Il D.p.s. cos'è?

Il D.P.S. è l'unico documento in grado di attestare l'adeguamento alla normativa sulla tutela dei dati personali (privacy) e la scadenza per la redazione è fissata al 31 di marzo di ogni anno. Il DPS è un manuale per la pianificazione della sicurezza dei dati in azienda: descrive come si tutelano i dati personali di dipendenti, collaboratori, clienti, utenti, fornitori ecc. Una delle più importanti novità introdotte con il Testo unico consiste nell'obbligo di riportare nella relazione accompagnatoria di bilancio d'esercizio, se dovuta, l'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

La videosorveglianza: la privacy nella gestione degli impianti audiovisivi

Per gli impianti audiovisivi sono state confermate tutte le norme precedenti ed in particolare il riferimento a quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300 (statuto dei lavoratori).

Stiamo parlando, principalmente, delle attività di videosorveglianza. Questa attività di trattamento di dati personali (ricordiamo ... anche le immagini possono costituire dati personali!) è stata oggetto di un approfondito studio da parte del Garante.

Uno studio che ha portato all'emanazione di un apposito comunicato in tema di videosorveglianza e che è stato pubblicato nel mese di Aprile del 2004.

In questo comunicato, semplice e molto esaustivo, viene disciplinata la videosorveglianza in tutte le sue ipotesi: dal controllo di aree esterne a quelle non esterne, dalla semplice visione alla videoregistrazione ed alla loro conservazione.

Sempre in questo comunicato viene disciplinata rigidamente la questione dell'informativa da rendere ad ogni interessato.

Tutela delle informazioni indesiderate ...

Con Il Codice Privacy è stata rafforzata la tutela contro le comunicazioni indesiderate (spamming), ribadendo il principio dell'opt-in (il consenso degli interessati), per cui è consentito l'invio di comunicazioni mediante sistemi automatizzati (posta elettronica, fax, dispositivi automatici di chiamata) solo dopo che l'interessato abbia dato il suo consenso esplicito: tale tutela è stata estesa anche all'invio di messaggi pubblicitari tramite Sms e Mms.

Localizzare i cellulari ...

Tra le novità più importanti introdotte dal Codice, vi è la tutela del trattamento dei dati relativi alla localizzazione dei cellulari.

Alle aziende erogatrici è vietato trattare dati che consentano di identificare il posizionamento di un utente (dati basilari, per esempio, per le attività di geomarketing) senza che lo stesso abbia dato il suo preventivo consenso, che è peraltro revocabile in ogni momento.

Giornalisti ...

Omissione delle generalità, pubblicazione di dati personali e di foto di detenuti (in manette) solo in caso di rilevante interesse giornalistica e solo dietro autorizzazione dell'interessato.

È vietato pubblicare dettagli su violenze commesse violando la dignità delle persone ed è vietato far riferimento allo stato di salute rispettando il diritto alla riservatezza e al decoro personale.

Absolute divieto nel rivelare particolari della vita privata di soggetti che non abbiano interesse giornalistico, quindi... sono banditi i pettegolezzi e le riprese con teleobiettivi che campeggiano nei giornali scandalistici.

Il cronista può avere un archivio personale perché lo stesso non può essere equiparato a una banca dati; stesso discorso vale per gli archivi delle redazioni dei giornali che però debbono due volte l'anno pubblicare un annuncio con l'indicazione del luogo dell'archivio, offrendo anche la possibilità di consultarlo.

I giornalisti non sono soggetti a nessun tipo di censura e - altra novità - in caso di effettiva e reale necessità possono non rilevare la loro identità nel caso in cui questo serva all'acquisizione di notizie per la realizzazione di inchieste, articoli e approfondimenti, oppure in gravi casi di pericolo per la loro incolumità.

Possiamo fare Ricorso al Garante?

Sono state riviste anche le norme relative ai ricorsi davanti al Garante, i quali possono essere comunicati dai singoli cittadini in varie fattispecie, per esempio proprio in caso di comunicazioni indesiderate.

Perché mettersi in regola

È obbligatorio ...

E' assolutamente obbligatorio essere in regola. Si rischiano sanzioni molto rigide: multe e reclusione, risarcimento del danno patrimoniale e morale ex art. 2050.

Alcune motivazioni per adeguarsi, subito!

La legge sulla Privacy e' pienamente vigente al pari di ogni altra legge dello Stato Italiano dal 01/01/2004. In caso di inadempienze accertate, si prevedono sanzioni di tipo amministrativo (fino a quasi 124.000 Euro) e la reclusione (fino a 3 anni), esclusione dalle gare di appalto, risarcimenti per danni.

L'Autorità Garante emana provvedimenti, effettua accertamenti e sanziona gli inadempimenti, di recente insieme alla Guardia di Finanza (sulla base di un accordo). È appropriato valutare, oltre che alle perdite economiche, anche ai danni che ricadono sull'immagine.

La tutela e protezione della privacy rientra negli allegati dell'avviso dell'e-government, nei progetti di qualità e negli accreditamenti istituzionali. La legislazione sulla privacy, considerata la velocità della crescita della tecnologia, e' destinata a rivestire un ruolo fondamentale.

Chi deve adeguarsi ...

Devono adeguarsi tutti coloro che trattano dati personali, ovvero, i seguenti soggetti:

- √ Aziende
- √ Professionisti
- √ Cooperative
- √ Associazioni
- √ Pubblica Amministrazione
- √ Scuole Pubbliche e Private
- √ Ospedali ed altri enti di assistenza e ricovero
- √ Enti pubblici ecc. (ovvero chiunque tratti dati personali di clienti, cittadini, dipendenti, fornitori, utenti, pazienti, colleghi, soci, associati ecc.).

Precisiamo che gli adempimenti variano a seconda delle dimensioni della struttura e della tipologia dei dati trattati.

Quali dati sono personali ...

- √ Il nome, il cognome, l'indirizzo, il numero di telefono, il codice fiscale, la partita iva, etc.
- √ Informazioni circa la composizione del nucleo familiare, la professione esercitata da un determinato soggetto, sia fisico che giuridico, la sua formazione...

- √ Fotografie, radiografie, video, suoni, impronte...
- √ Informazioni relative al profilo creditizio, alla retribuzione...
- √ Informazioni relative alla salute di un soggetto, alla vita sessuale
- √ Partecipazione ad associazioni di categoria, a partiti
- √ Trattenute sindacali
- √ Cartelle cliniche
- √ Rilevazioni di presenze
- √ Curriculum vitae di dipendenti, collaboratori o candidati...

Infatti, una ditta individuale che non si avvale di nessun collaboratore, sarà gravata da diversi adempimenti rispetto ad una struttura societaria.

Da cosa si differenziano gli adempimenti ...

- √ Dimensione e tipologia di struttura che effettua il trattamento dei dati
- √ Dal tipo di dati trattati
- √ Dalle modalità di trattamento
- √ Dall'esistenza o meno di una struttura informatica collegata ad internet

Come adeguarsi!

- √ Nominando le figure richieste dalla legge
- √ Proteggendo gli elaboratori contro il rischio di intrusione e di virus
- √ Adottando le misure fisiche di protezione (allarmi, stabilizzatori di corrente, armadi chiusi a chiave ed ignifughi, accesso selezionato ai locali...)
- √ Mettendo per iscritto le procedure da seguire e soprattutto di redigere il D.P.S. (Documento Programmatico sulla Sicurezza), una documentazione che descrive quanto fatto ed individua quanto ancora resta da fare. Solo il D.P.S. fa prova dell'avvenuto adeguamento alla normativa
- √ Programmando un adeguamento progressivo, che non resti lettera morta
- √ Inventariando i dati personali, adottando le misure di sicurezza obbligatorie (fisiche, logiche ed organizzative), adeguandosi agli obblighi di informativa, consenso, nomina figure, redigendo il Documento Programmatico sulla Sicurezza

Controlli: Il Garante e la Guardia di Finanza ...

E' stato emanato a Roma un protocollo di collaborazione tra la Guardia di Finanza ed il Garante della Privacy. L'accordo ha l'obiettivo di regolare le reciproche forme di intesa finalizzate a porre in essere una sempre più intensa ed efficace attività di controllo sulla raccolta dati. In particolare, la Guardia di Finanza collabora alle attività ispettive attraverso la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento lo sviluppo di attività delegate o sub-delegate per l'accertamento delle violazioni di natura penale ed amministrativa. Inoltre, il Corpo, collabora nell'esecuzione di indagini conoscitive sullo stato di attuazione della legge in determinati settori. L'Autorità ha attivato il "Nucleo Speciale Servizi Extratributari della Guardia di Finanza" il quale assicura, con proiezioni

su tutto il territorio nazionale, avvalendosi anche della collaborazione dei Nuclei di Polizia Tributaria territorialmente competenti.

I rischi?

Sanzioni a seguito di controllo ispettivo (recentemente una parte della Guardia di Finanza é stata distolta dalle funzioni ordinarie per occuparsi di privacy): si rischiano la reclusione e sanzioni pecuniarie fino a 124.000 Euro. La casistica della violazioni che danno diritto a risarcimento del danno è molto varia.

L'art. 2050 c.c. qualifica il trattamento dei dati come attività pericolosa.

A livello pratico significa che chi tratta i dati, per evitare ogni responsabilità, deve dimostrare di aver adottato "tutte le misure idonee ad evitare il danno".

Significa dunque che il titolare dei dati deve dare prova (documentata, vedi Documento Programmatico Sulla Sicurezza) di aver adottato tutte le misure di sicurezza nella miglior versione possibile.

Le sanzioni ...

Il Garante tiene ad una precisa applicazione della normativa contenuta nel Codice.

Il suo operato si ispira ad un'idea di massima tutela e protezione dei dati personali a favore dell'interessato.

Viene vista, e noi ne siamo fortemente convinti, come una profonda questione morale tanto che, chi trasgredisce, è soggetto a pene molto, ma davvero molto severe.

Infatti, giusto per elencarne qualcuna:

- √ Multe da 3.000 a 50.000 euro, elevabili al triplo
- √ Reclusione fino a 3 anni
- √ Possibilità di estinguere il reato penale, adeguandosi alla normativa e pagando una sanzione pecuniaria
- √ Risarcimento del danno cagionato ex art. 2050

Chi deve dar prova ...

Non è l'interessato a dover provare il danno ma colui che l'ha provocato a dover dimostrare di aver fatto tutto il possibile per evitarlo.

Questa procedura civilistica viene definita "inversione dell'onere della prova".

Ecco perché insistiamo fortemente sulla redazione e sul continuo aggiornamento del D.p.s. che, come dicevamo prima, è l'unico atto che può formalmente attestare il nostro operato in materia di applicazione delle misure di sicurezza e quant'altro previsto dal Codice!

Attività pericolosa?

L'art. 2050 c.c. parla di "attività pericolosa" (elevata potenzialità di danno, per la natura dell'attività o dei mezzi di lavoro utilizzati).

Il trattamento dei dati viene dunque distinto come esercizio di attività pericolosa. Da questa denominazione proviene un'importante conseguenza circa l'onere della prova. Di solito chi si ritiene danneggiato da un fatto illecito, deve provare la responsabilità di colui che ha commesso il fatto.

Nell'ipotesi regolata dall'art. 2050 è sancito invece il "principio dell'inversione dell'onere della prova". Quindi noi danneggiati dobbiamo solo provare il fatto storico, mentre colui che effettua il trattamento, e che ha causato il danno, deve dimostrare di aver adottato tutte le misure idonee ad evitarlo.

La prova è molto importante, dobbiamo, infatti, dimostrare una prova positiva di aver impiegato ogni cura o misure atte ad impedire l'evento dannoso, in caso contrario dobbiamo riparare al danno

Gli errori commessi dai dipendenti ...

La legge 547/93 ha introdotto nel nostro ordinamento vari "crimini informatici", ovvero l'attentato a impianti informatici di pubblica utilità, falsificazione di documenti informatici, accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, violazione di corrispondenza telematica, intercettazione di e-mail, danneggiamento di sistemi informatici o telematici (...).

Il datore di lavoro rischia di essere ritenuto in concorso con il dipendente a lui subordinato che ha commesso il crimine informatico, per non aver posto in essere tutte le misure di prevenzione e controllo idonee a garantire la sicurezza del trattamento dei dati.

La mancata adozione di tutte le misure idonee a ridurre al minimo i rischi viene considerata difatti un'agevolazione alla commissione del crimine.

Chi paga il danno ...

I soggetti tenuti al risarcimento dei danni causati dal trattamento dei dati personali, sono il "titolare" (ossia colui "cui competono le decisioni in ordine alle finalità del trattamento" e "della sicurezza") ed il "responsabile" (ossia colui che è preposto dal titolare al trattamento dei dati, avendo "esperienza, capacità ed affidabilità" tale da fornire "idonea garanzia del pieno rispetto delle disposizioni di legge in materia di trattamento, ivi compreso il profilo relativo alla sicurezza").

L'Allegato B (Disciplinare Tecnico)

Trattamenti con strumenti elettronici

Questa volta ci è piaciuto davvero: infatti il Garante non solo ha dettato le norme, ma ha anche disposto, nell'allegato B), un vero e proprio piano per gestire al meglio la privacy: ecco, ora, le modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

- √ Il trattamento di dati personali con strumenti elettronici e' consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
- √ Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
- √ Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
- √ Con le istruzioni impartite agli incaricati e' prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
- √ La parola chiave, quando e' prevista dal sistema di autenticazione, e' composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed e' modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi.
- √ In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave e' modificata almeno ogni tre mesi.
- √ Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
- √ Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- √ Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- √ Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
- √ Quando l'accesso ai dati e agli strumenti elettronici e' consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali e' organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
- √ Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

- √ Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso e' utilizzato un sistema di autorizzazione.
- √ I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
- √ Periodicamente, e comunque almeno annualmente, e' verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
- √ Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
- √ I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
- √ Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento e' almeno semestrale.
- √ Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
- √ Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
 - √ l'elenco dei trattamenti di dati personali
 - √ la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati
 - √ l'analisi dei rischi che incombono sui dati
 - √ le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità
 - √ la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
 - √ la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione e' programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali
 - √ la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare
 - √ per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Altre misure in caso di trattamento di dati sensibili o giudiziari

- √ I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
- √ Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
- √ I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
- √ Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
- √ Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

- √ Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
- √ Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
- √ Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici

Trattamenti senza l'ausilio di strumenti elettronici

- √ Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

- √ Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone sprovviste di autorizzazione, e sono restituiti al termine delle operazioni affidate.
- √ L'accesso agli archivi contenenti dati sensibili o giudiziari e' controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Conclusioni

Certo, così come detto nelle prime pagine, non è tutto ma siamo contenti di avervi dato l'opportunità di farti un'idea della privacy e di questo ti ringraziamo ... avendolo letto.

Operiamo nell'ambito dei servizi reali rivolti alle imprese sia di natura pubblica che privata e, nel corso di anni di intensificate esperienze, ci offriamo al mercato imprenditoriale e professionale con una gamma di servizi che garantiscono un ottimo rapporto qualità/prezzo e di interessante valore.

Nel caso in cui avessi difficoltà in termini normativi e procedurali ... puoi contattarci ai recapiti di cui in introduzione senza impegni da parte Vostra nei nostri confronti.

Buon Lavoro!
Brixia Business Solutions

Brixia Business Solutions

Via Enrico Berlinguer n. 5 - 84010 San Marzano Sul Sarno (Sa - Italia)

Tel et Fax **081 5186174 - 081 5187648** - Cp Mobile **389 6804697**

Posta elettronica : contatti@brixia.info