Privacy: cosa fare?

La normativa sulla privacy ha lo scopo di proteggere e di evitare la diffusione dei dati personali.
Per dati personali s'intendono i dati delle persone fisiche.
Obiettivo della normativa è garantire a coloro che affidano i loro dati personali a soggetti terzi che questi siano adeguatamente protetti al fine di evitarne un uso improprio, illecito o non autorizzato.
La norma prevede che i dati personali vadano trattati con particolare cura, una maggiore attenzione andrà posta verso il trattamento di dati sensibili o giudiziari:
i dati sensibili sono quelli relativi a malattie, stato di salute, razza, scelte politiche, religiose o ideologiche, ecc.;
i dati giudiziari sono quelli relativi ai reati, carichi pendenti, ecc..

Chi deve mettersi in regola: TUTTI, ma gli adempimenti da recepire variano da caso a caso
Ogni attività lavorativa tratta dati personali ed ha archivi cartacei e/o strumenti elettronici relativi ai propri clienti, fornitori, collaboratori e spesso anche di terzi, basti pensare a:

- dati anagrafici
- fatture di spesa e d'incasso
- documenti di trasporto
- corrispondenza
- atti di proprietà
- dati catastali
- cartigli dei disegni
- perizie
- fotografie
- ricevute mediche
- buste paga
- contratti

Anche un piccolo negozio, un artigiano, lo studio di un singolo professionista senza collaboratori e addirittura senza computer deve adeguarsi e avere un minimo di misure previste.

Le figure previste:

Il titolare del trattamento dati
Il titolare del trattamento dati non dev'essere confuso con il "titolare" (generalmente il socio unico o l'amministratore delegato) della società. Secondo il Codice della Privacy, infatti, il "Titolare" è l'ente, l'organizzazione, l'azienda nel suo complesso.

Il responsabile del trattamento dati
È una figura prevista dal Codice della Privacy, la cui nomina, però, è sempre facoltativa. Di solito se ne raccomanda l'adozione per realtà aziendali più importanti, imprese medio/grandi con un elevato numero di dipendenti, non inferiore a 15. I Responsabili del Trattamento, in un'azienda possono anche essere più d'uno, devono essere nominati per iscritto e rispondono al Legale Rappresentante.

L'amministratore di sistema
È assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi *software* complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. Nel caso di sufficienti (e comprovate) capacità informatiche potrà essere anche il legale rappresentante o un consulente informatico. La nomina è sempre obbligatoria, ad eccezione dei casi in cui amministratore di sistema e legale rappresentante siano la stessa persona o nei casi in cui l'amministratore di sistema sia un soggetto esterno all'azienda (consulente informatico o dipendente di altra società).

Gli incaricati del trattamento
Sono le persone fisiche che trattano o possono accedere ai dati, sia cartacei sia informatizzati. Devono essere nominate per iscritto.
Nel caso del singolo professionista o titolare senza collaboratori evidentemente le varie figure (titolare, amministratore di sistema e incaricato) corrisponderanno alla stessa persona. Secondo le dimensioni della propria organizzazione e le capacità personali i vari ruoli possono coincidere in una o più persone o dividersi tra più persone, ma comunque definite e nominate.

Le nomine
Tutte le figure previste dal "mansionario privacy", con la sola eccezione del Titolare del Trattamento (e del "Legale Rappresentante"), devono ricevere una nomina per iscritto. L'atto di nomina è un atto che, ai sensi del Codice Civile, ha natura contrattuale e che, perciò, necessita della firma di accettazione da parte della persona nominata. In mancanza della firma, il contratto non si perfeziona e la nomina non produce effetti legali.

L'informativa sulla privacy
La norma prevede che per trattare i dati personali di chiunque bisogna sempre informare l'interessato. L'informativa, salvo rarissime eccezioni (ad esempio per far valere un proprio diritto in sede giudiziaria) è sempre necessaria, tuttavia può essere fornita anche in forma orale.

Il consenso al trattamento
Nella stragrande maggioranza dei casi, per poter effettuare un trattamento di dati personali, è necessario ricevere il consenso preventivo da parte dell'interessato. Ci sono però delle eccezioni, ad esempio quando i dati derivano da un rapporto contrattuale (come per i clienti, fornitori, collaboratori); quando i dati personali derivano da pubblici registri come i siti Internet o simili o quando vanno trattati per un obbligo di legge. In molti casi, inoltre, il consenso può essere espresso oralmente (ma registrato per iscritto). Il consenso dev'essere espresso per iscritto solo quando riguarda il trattamento di dati sensibili.
Non è più richiesto alcun consenso specifico al trattamento per i "curricula"richiesti o spediti dai candidati alle aziende, anche se contengono dati sensibili. Solo nel caso in cui il candidato viene convocato per un colloquio è necessario fornirgli, in tale sede, una sintetica informativa.
Perdono lo status di "dati personali" i dati delle persone giuridiche. L'esenzione non copre i trattamenti per finalità di promozione commerciale, ma ha un importante impatto: Non vi è più l'obbligo di fornire informativa privacy a fornitori e clienti, se questi ultimi sono aziende od enti. Vi ricordiamo che tale esenzione non è retroattiva ma decorre dal 7 dicembre 2011.

La cancellazione dei dati

Chiunque può chiedere al professionista, al titolare, al fornitore, alla società,ecc., se tratta i propri dati, la rettifica, l'aggiornamento, il blocco o la cancellazione per questo la normativa prevede che sia utilizzato un software con i dati personali per garantire una veloce ricerca e cancellazione.

Nel caso in cui una persona fisica o giuridica richieda il blocco dei dati sarà necessario rendere i dati dell'interessato non più utilizzabili dal software e spostare tutti i documenti in armadi chiusi a chiave e inaccessibili, per essere utilizzati solo per obblighi di legge o per tutela giuridica.

E' obbligatorio rilasciare un attestato sull'avvenuta cancellazione, blocco o rettifica dei dati personali.

L'archivio cartaceo

La normativa stabilisce semplici regole per la gestione degli archivi cartacei, prevede solo che vengano adottate e comunicate ai vari operatori le norme d'accesso.

Per i normali dati cartacei sono sufficienti le classiche scaffalature a giorno con i faldoni, i contenitori a bottone, i tubi per i disegni, ecc., l'importante è che non siano in luoghi aperti al pubblico o non presidiati, e ovviamente non bisogna scrivere sulla costa dei faldoni dati personali come il nome del cliente, basta scrivere un codice identificativo o il nome del progetto, ad esempio scrivere PROGETTO n°xxxx oppure PRATICA VIA xxxx ma non PRATICA MARIO BIANCHI o PRATICA VIA MILANO 45.

Se gli archivi sono invece in una sala d'aspetto non controllata a vista o in un corridoio di passaggio allora è opportuno che gli armadi siano chiusi a chiave.

E se si trattano anche dati sensibili o giudiziari?

Alcune attività non hanno dati sensibili o giudiziari ma solo dati personali generici, ma ad esempio nel caso di dipendenti le buste paga e i documenti sanitari contengono dati sensibili in quanto consentono di risalire allo stato di salute.

Per quest'ultimi basta avere un armadio chiuso a chiave o un ripostiglio con una porta con la serratura, e avere un registro dove scrivere chi ha preso cosa e quando. E' necessario l'utilizzo di un distruggi-documenti per tutti i documenti con dati personali sensibili o giudiziari da cestinare.

La sicurezza dei luoghi

Ovviamente i dati personali, sia nei computer che negli archivi, devono essere in un luogo accessibile solo ai vari operatori (ad esempio il proprio studio, negozio o laboratorio, come normalmente avviene) e bisogna adottare alcune misure di sicurezza passive o attive, come la porta blindata, grate alle finestre, sistema antifurto e quant'altro, quando necessario. Non ci sono regole precise, basta garantire uno standard minimo di sicurezza contro eventuali intrusioni.

Ovviamente le misure dovranno essere proporzionate al tipo di dati posseduti. Non ha senso fare un caveau per le fatture di spesa, ma chiudere a chiave l'ufficio quando ci si assenta è sicuramente opportuno.

Stampanti e fax devono essere posizionate in luoghi presidiati e non accessibili al pubblico per evitare che vengano letti dati personali, anche del tutto casualmente. Nel caso di studi associati che utilizzano attrezzature in comune è necessario garantire reciprocamente il rispetto della privacy in forma scritta.

Il commercialista

Molti trasmettono all'esterno i propri dati contabili al commercialista.

In ogni caso i dati personali sono solo affidati al commercialista e rimangono sempre sotto la propria tutela quindi è necessario verificare che operi in conformità alla normativa sulla privacy e

che rilasci una garanzia scritta sull'applicazione della normativa e un obbligo di riservatezza sui dati stessi.
Nel caso qualcuno risalisse a dati personali tramite il commercialista, magari per sapere informazioni sullo stato dei pagamenti o sulla solvibilità economica di un cliente, ne siete comunque direttamente responsabili. Considerate che il commercialista, spesso, tratta anche dati sensibili, come la scelta a chi destinare "l'otto per mille".

L'impresa di pulizie
Normalmente l'impresa di pulizie lavora al di fuori dell'orario di lavoro e anche non volontariamente è possibile che vengano letti dati personali.
Anche l'impresa deve rilasciare una garanzia scritta sul non utilizzo dei dati che possono essere letti, sull'applicazione della normativa e un obbligo di riservatezza sui dati stessi, oltre a fornire l'elenco (aggiornato almeno annualmente) delle persone fisiche autorizzate ad accedere ai locali dei propri clienti.

Email e Fax
Ovviamente è possibile inviare email e fax ai propri clienti e fornitori senza chiedere ulteriori consensi agli stessi ma per inoltrare informative email o fax ad esempio per ricercare futuri clienti o comunicare i servizi offerti, bisogna sempre prima chiedere il consenso all'invio.

Il trattamento informatizzato dei dati
Tutte le attività ormai utilizzano computer per trattare dati personali, basti pensare ai file di fatture o relazioni, ai disegni degli architetti, agli atti dei notai, alle domande al Comune o al Catasto e così via, tutti documenti dove sono riportati dati personali.
La normativa sulla privacy prevede regole chiare e precise per la gestione dei dati quando sono informatizzati:
Ma sono semplici regole di utilizzo.
- Usare sempre password di almeno 8 caratteri per accedere ai computer
- Cambiare le password periodicamente (almeno ogni 90 giorni)
- Fare periodicamente il backup dei dati (almeno una volta la settimana)
- Effettuare, almeno una volta all'anno, un "test di ripristino"
- Stabilire procedure di archiviazione e di sicurezza
- Utilizzare (e aggiornare) antivirus e firewall
- Determinare procedure di utilizzo dei computer, della rete dati e di Internet (come ad esempio attivare il salvaschermo del computer con la riattivazione con password)
- Stabilire chi è responsabile e di che cosa
Niente di più che quello che un'attività moderna e ben organizzato già fa (chi vorrebbe perdere i dati di un progetto su cui ha lavorato per mesi, magari per un virus o per non aver fatto il backup?)

La Notificazione al Garante
In rari casi, quando i dati sono particolarmente sensibili (ad esempio per i dati genetici, dati biometrici, dati ai fini della procreazione assistita, dati per la selezione del personale conto terzi, dati per la valutazione della ecc.), va fatta la Notificazione del Trattamento al Garante. Si tratta di una procedura (a pagamento) che può essere effettuata esclusivamente via Internet sul sito del Garante per la Privacy.

Gli Amministratori di Sistema

Un recente provvedimento del Garante (del 27 novembre 2008) ha introdotto dei nuovi obblighi per i Titolari che dispongono di almeno un amministratore di sistema diverso dal legale rappresentante. Dal recepimento di tali obblighi, tuttavia, sono esonerati i soggetti che non trattano i dati sensibili dei propri clienti, purché si tratti di aziende con meno di 250 dipendenti.

Per chi invece è soggetto al nuovo provvedimento, gli adempimenti richiesti sono sostanzialmente quattro:

- Nomina, per iscritto, di ogni singolo amministratore di sistema;
- Redazione e aggiornamento (almeno annuale) dell'elenco degli amministratori di sistema;
- Registrazione, mediante apposita soluzione informatica, degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni devono avere caratteristiche di completezza ed inalterabilità. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo non inferiore a sei mesi;
- L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti. Di tale attività dev'essere data evidenza mediante la redazione di un'idonea relazione scritta annuale.

I Documenti

La norma prevede che non debba essere presentato o consegnato alcun documento a nessun ente o autorità.

In effetti è sufficiente conservare ed aggiornare periodicamente:

1. le informative sulla privacy (eventualmente comprensive di consenso al trattamento);
2. le lettere di nomina degli incaricati (e, eventualmente, dei responsabili e degli amministratori di sistema);
3. l'elenco (aggiornato annualmente) degli incaricati al trattamento dei dati (e, eventualmente, degli amministratori di sistema);
4. le lettere di "garanzia" nei confronti dei fornitori terzi che trattano dati personali per conto del titolare (ad esempio: le società che si occupano di paghe e contributi, o le società che effettuano le pulizie nei locali dell'azienda);

Solo la Notificazione al Garante, se prevista, deve essere effettuata via Internet al Garante.

Le sanzioni

Le sanzioni sono molto salate: si parte da un minimo di €6.000 sino ad un massimo di €180.000, ma queste sono soltanto le sanzioni amministrative, cui vanno aggiunti gli eventuali illeciti penali (fino a tre anni di reclusione) e gli eventuali risarcimenti, in ambito civile, per gli interessati "danneggiati" dal trattamento illecito dei loro dati.

I controlli sono affidati al Garante per la Privacy e alla Guardia di Finanza.

** le parti in corsivo sono parte integrante delle semplificazioni introdotte con il Decreto Legge n.201 del 6 dicembre 2011.*