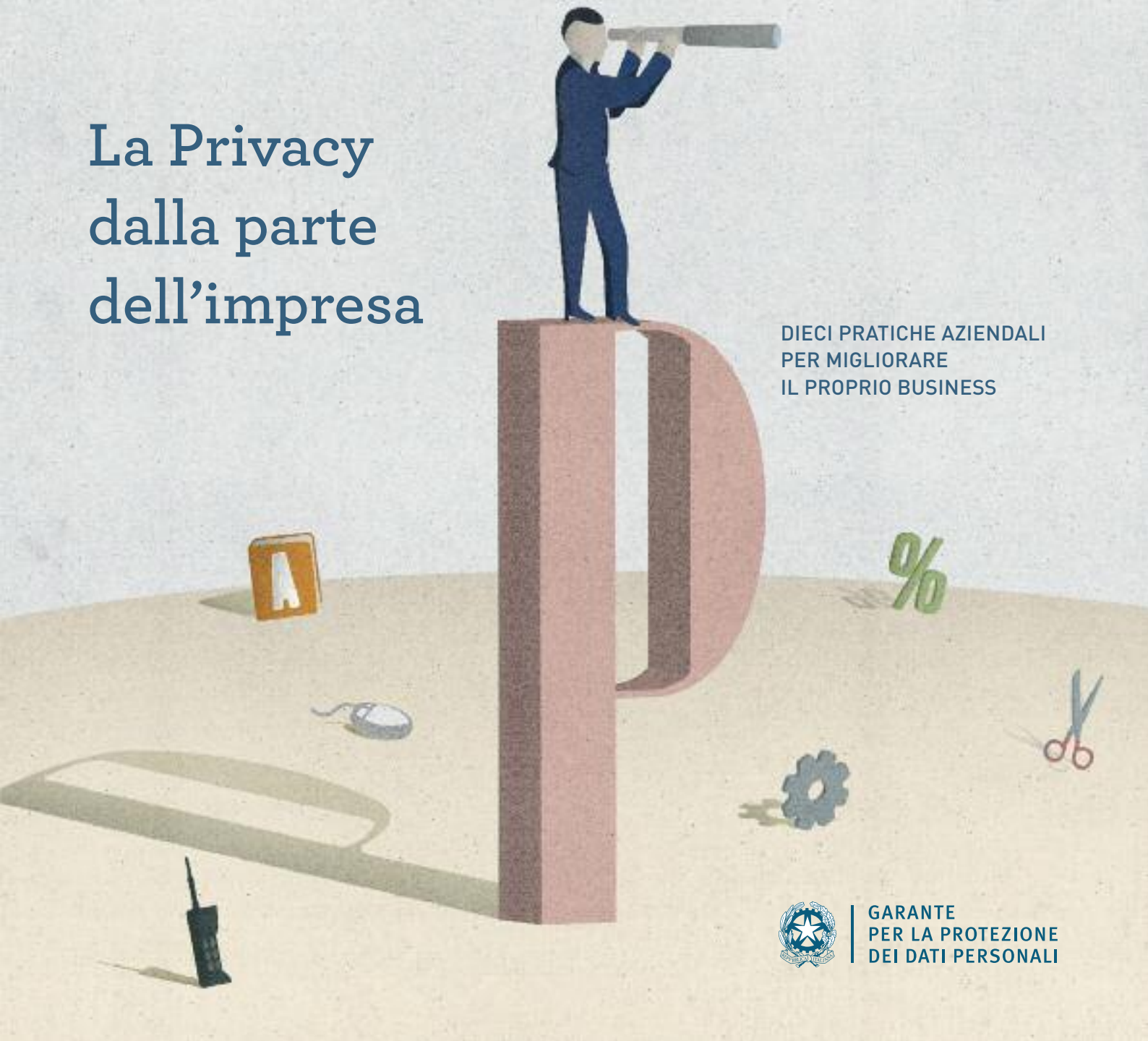
La Privacy dalla parte dell'impresa

DIECI PRATICHE AZIENDALI
PER MIGLIORARE
IL PROPRIO BUSINESS



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Premessa

La privacy, da costo a risorsa

La tutela della privacy è un diritto fondamentale della persona e una necessità imprescindibile della società moderna. Tuttavia viene spesso vissuta e interpretata in ambito imprenditoriale come un obbligo burocratico che rallenta o rende più macchinoso il raggiungimento degli obiettivi d'impresa.

Ciò anche perché non sempre gli operatori sono a conoscenza delle opportunità e delle modalità semplificate che il Garante ha, nel tempo, indicato per ottenere una conformità sostanziale alla protezione dei dati, evitando il ricorso ad adempimenti inutili e meramente formali.

Da un'attenta analisi delle prassi aziendali emerge, tra l'altro, che la corretta adozione di semplici misure a protezione dei dati personali può contribuire a rendere più efficiente l'organizzazione dell'impresa e a ridurre sensibilmente i potenziali rischi a cui la stessa si espone sul mercato.

Nello spirito di collaborazione con il mondo imprenditoriale, il Garante della privacy ha voluto così evidenziare una selezione di dieci *"best practice"* che possono migliorare non solo l'immagine dell'impresa, come soggetto attento al principio di "responsabilità sociale", ma anche la capacità di business a parità di costi sostenuti, aumentando la fiducia di utenti e consumatori nella serietà e affidabilità dell'impresa.

Questa breve guida ha lo scopo di offrire alcuni spunti di riflessione e soprattutto poche ma fondamentali regole e consigli pratici, affinché gli investimenti iniziali necessari per proteggere i dati vengano opportunamente raffrontati con i numerosi benefici diretti e indiretti da essi generati.

Chi desidera approfondire aspetti giuridici in materia di privacy accennati in questa guida o cerca riferimenti puntuali sugli adempimenti previsti nel proprio settore d'impresa può consultare l'apposita documentazione e i provvedimenti pubblicati sul sito **www.garanteprivacy.it**

L'Autorità è comunque sempre a disposizione per risolvere eventuali dubbi o trovare le soluzioni più adeguate.

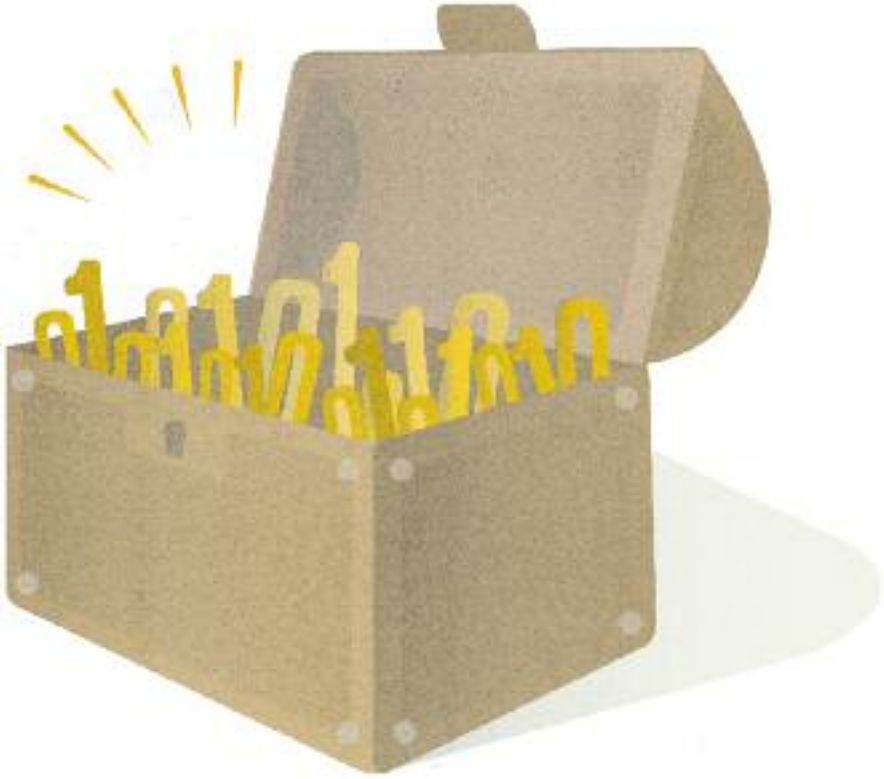
1 Il valore dei dati

Nella società dell'informazione, i "dati" rappresentano spesso uno dei beni più preziosi posseduti da un'impresa, sia essa di grandi o piccole dimensioni. Possono essere di tipo commerciale, rappresentare il portafoglio degli attuali clienti o di quelli futuri, raccontare l'organizzazione interna e l'attività di ricerca e sviluppo. Qualunque manager ne conosce l'importanza e cerca di usarli al meglio. Non bisogna dimenticare, però, che le potenzialità economiche dei dati sono direttamente proporzionali alla liceità del loro trattamento: raccoglierli nel rispetto della privacy, e poterne quindi liberamente usufruire, significa creare valore per l'azienda. È bene, tra l'altro, che la *leadership* di un'azienda sia ben consapevole della differenza esistente tra i vari tipi di dati. Alcuni infatti possono essere utilizzati senza particolari problemi, altri necessitano di apposite garanzie e protezioni.

I **dati personali** sono tutte le informazioni relative a una persona fisica, identificata o identificabile, anche indirettamente (mediante riferimento a qualsiasi altra informazione), incluso l'eventuale numero di identificazione personale. Dati personali sono, ad esempio, un indirizzo e-mail o l'immagine fotografica di una persona, il codice fiscale o un numero telefonico, un indirizzo IP o una targa automobilistica. Si ricorda che, in base a una recente novità legislativa, non sono più considerati come dati personali, e quindi, almeno in linea generale, non sono più tutelati dalla normativa sulla privacy, i dati riferibili alle persone giuridiche, ovvero a imprese, enti e associazioni.

I **dati sensibili** sono quei particolari dati personali che consentono di rivelare l'origine razziale ed etnica di una persona, le sue convinzioni religiose, filosofiche o di altro genere. Lo sono anche quelli che indicano l'adesione a partiti, sindacati, associazioni od organizzazioni

a carattere religioso, filosofico, politico o sindacale. Oppure i dati idonei a rivelare lo stato di salute e la vita sessuale. Sono tutte informazioni delicate che possono incidere sulla riservatezza e la dignità dell'individuo. Tra i dati che necessitano di particolari cautele vi sono quelli **giudiziari** - una categoria che include fra l'altro le informazioni contenute nel casellario giudiziale e quelle connesse alla posizione di imputato o indagato in procedimenti penali – ma anche i dati **biometrici** o i dati **genetici**.



2 A ciascuno le sue responsabilità

In un'azienda moderna la ripartizione dei compiti e delle responsabilità è definita con chiarezza. La struttura organizzativa può essere complessa, policentrica, ma per raggiungere gli obiettivi prefissati è comunque opportuno che emerga "chi fa cosa" e con quali scadenze.
La catena di comando è particolarmente importante anche quando i "beni" usati sono i dati personali. Il Codice della privacy evidenzia questa necessità e impone di definire bene quali figure hanno la possibilità di trattare dati personali.
Il **titolare del trattamento** (*data controller*) è il soggetto che esercita un potere decisionale, del tutto autonomo, sulle finalità e sulle modalità del trattamento. La qualità di titolare non può essere liberamente determinata dai contraenti ma discende direttamente dai poteri che si esercitano sui dati. Può essere sia una persona fisica (si pensi all'imprenditore individuale) sia una persona giuridica (ad esempio, una società a responsabilità limitata) che tratta i dati (con la raccolta, la registrazione, la comunicazione degli stessi o la loro diffusione).
Il titolare del trattamento, se lo ritiene utile in base all'organizzazione aziendale, può designare uno o più soggetti come **responsabile del trattamento** (*data processor*) ed è tenuto a vigilare sulla puntuale osservanza delle istruzioni impartite loro. La nomina deve essere effettuata con un atto scritto in cui siano precisati anche i compiti affidati. Occorre comunque scegliere persone fisiche od organismi (inclusi soggetti esterni all'impresa) che per esperienza, capacità e affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, compreso il profilo relativo alla sicurezza.
Sono molti i casi in cui l'azienda, per scelta o per necessità, fa svolgere parte delle attività e del conseguente trattamento dei dati a soggetti esterni.

Proprio in questi casi, a seconda del tipo di contratto che definisce tale rapporto, può essere non solo opportuno, ma necessario che l'azienda nomini il soggetto esterno quale responsabile del trattamento (ad esempio quando si utilizzano servizi informatici in *outsourcing* oppure quando ci si avvale dei servizi offerti da un *call center* o da un altro tipo di fornitori).

Gli **incaricati del trattamento** sono le persone fisiche che effettuano materialmente le operazioni di trattamento dei dati personali e operano sotto la diretta autorità del titolare (o del responsabile se è stato nominato) secondo precise istruzioni. Per poter svolgere queste operazioni in maniera lecita, è necessario che il personale chiamato a trattare i dati venga opportunamente designato per iscritto individuando puntualmente l'ambito di trattamento consentito. Al fine di semplificare questo adempimento è però sufficiente documentare l'inserimento di un soggetto in una determinata unità organizzativa (ad esempio l'ufficio del personale oppure l'ufficio vendite). Ciò a condizione che risulti, per iscritto, quale sia l'ambito di trattamento dei dati consentito agli addetti di tale unità.

3 Trasparenza e correttezza nel business

In generale è una regola di buon senso (spesso sancita dalla legge) quella che impone di informare il legittimo proprietario e di chiedere il suo permesso prima di utilizzare un bene che gli appartiene. Tale accortezza consente di mantenere proficui rapporti personali e professionali. Se il bene in questione è un "dato personale", occorre rivolgersi alla persona fisica a cui si riferiscono i dati, ovvero all'**interessato**. Anche in questo caso, il Codice della privacy definisce con maggiore precisione le prassi di trasparenza e correttezza, contribuendo a facilitare i rapporti dell'impresa con i consumatori (e tutti gli interessati) e a prevenire eventuali contenziosi.

Informativa - la semplicità al primo posto

Un'impresa che tratti dati personali deve quindi spiegare agli interessati (ad esempio ai propri clienti e dipendenti), con un'**informativa completa e chiara**, le caratteristiche essenziali dei trattamenti effettuati: dove sono stati presi i dati, le finalità e le modalità del trattamento, se i dati debbano o possano essere forniti (ad esempio è necessario il conferimento dei dati per la fatturazione di un servizio, mentre è facoltativo fornire informazioni a fini di profilazione), i soggetti o le eventuali categorie ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza, nonché il nome di almeno un responsabile del trattamento, qualora designato.
È bene rimarcare che l'informativa deve essere per quanto possibile sintetica e comprensibile: meglio se espressa attraverso simboli o icone, specialmente nei vari contesti tecnologici, anziché attraverso testi lunghi e burocratici. Le imprese hanno grandi capacità di comunicazione che, se utilizzate, consentono di migliorare ulteriormente la trasparenza in questo campo.
Bisogna informare la persona

interessata prima di cominciare a utilizzare i suoi dati, ma tale comunicazione può avvenire anche a voce, ad esempio quando si ha la possibilità di un contatto diretto o telefonico, o interagendo con l'interessato anche mediante il sito web aziendale.
Proprio per permettere che questo importante compito non diventi un costo per le imprese, il Garante ha consentito e suggerito forme semplificate di informativa, adatte alle specifiche esigenze espresse da singoli imprenditori o dalle associazioni di categoria. Ad esempio, ferme restando le specifiche norme di tutela previste dallo Statuto dei lavoratori, per informare le persone dell'esistenza di un sistema di videosorveglianza in un supermercato è sufficiente esporre dei cartelli che segnalino le telecamere e che indichino le finalità della ripresa e il nome del responsabile del trattamento a cui rivolgersi per eventuali informazioni aggiuntive.
Per avvisare che un veicolo aziendale è sottoposto a geolocalizzazione si può, ad esempio, fornire una prima informativa semplificata applicando un apposito adesivo (vetrofania) ai vetri della vettura. Un call center che offre assistenza ai clienti può proporre un breve messaggio preregistrato per informarli sul trattamento dei loro dati prima della fornitura del servizio (ne sono un esempio i messaggi proposti dalle centrali radio taxi).

In casi particolari, il singolo imprenditore o la stessa associazione di categoria possono rivolgersi al Garante per chiedere un esonero o per definire ulteriori procedure semplificate nel caso in cui, ad esempio, si debba contattare un numero molto elevato di persone difficilmente raggiungibili. Se l'informativa individuale richiede mezzi sproporzionati, l'Autorità può così autorizzare anche la sola pubblicazione dell'informativa su un sito internet o altri media, magari rinviando la comunicazione individuale al primo contatto utile con l'interessato.

Consenso

L'impresa, dopo aver informato l'interessato, deve in genere chiedergli il consenso per utilizzare i suoi dati personali: tanto che si parla di **consenso** "informato". Tale consenso, affinché il trattamento dati svolto possa considerarsi legittimo, deve essere liberamente espresso, evitando quindi di adottare condizionamenti o pressioni per ottenerlo, documentato per iscritto (se è stato espresso a voce, ad esempio, si può tenere traccia da chi, dove e quando sia stato ottenuto il consenso). È anche necessario differenziare il consenso richiesto in base allo specifico tipo di trattamento

che si vuole effettuare, eventualmente spiegando alla persona interessata - ad esempio un cliente - quali benefici può avere offrendo il suo assenso al trattamento dei dati (servizi personalizzati, offerte di prodotti particolari o vantaggi commerciali...).
A tal proposito, è bene ricordare che l'utilizzo dei dati personali per finalità di marketing non può essere reso di fatto obbligatorio, condizionando ad esempio l'accesso ai contenuti informativi di un sito web al rilascio del consenso a trattare i dati per finalità diverse, quali la profilazione e il marketing.
Occorre fare attenzione anche quando si acquisiscono liste di dati personali da soggetti terzi e non direttamente dagli interessati: prima di utilizzarli è infatti necessario verificare se gli interessati abbiano dato il proprio consenso (magari con verifiche a campione sui dati acquistati) al tipo di trattamento dati che si vuole svolgere, come quello per l'invio di offerte commerciali.
L'azienda dovrà poi ricordarsi di fornire l'informativa alle persone interessate già al momento della registrazione o del primo utilizzo dei loro dati.

Consenso non necessario - alcuni esempi

Il Codice della privacy e le ulteriori semplificazioni introdotte dal Garante prevedono numerosi casi in cui non è richiesto il consenso delle persone interessate - siano esse clienti o dipendenti, fornitori o semplici utenti - affinché l'impresa possa trattare i loro dati personali.
Naturalmente il consenso non è richiesto quando il trattamento è previsto da un obbligo di legge (come quello che impone agli alberghi di comunicare le generalità delle persone alloggiate alle autorità di pubblica sicurezza), da un regolamento o dalla normativa comunitaria.
Inoltre, il consenso non è necessario quando i dati vengono trattati per adempiere, prima della conclusione di un contratto, a specifiche richieste dell'interessato, come avviene per i dati

necessari per la concessione di un mutuo bancario (ad esempio la copia del preliminare di acquisto della casa). Il consenso non occorre neppure per il trattamento dei dati necessari per l'esecuzione di un contratto già in essere, come quelli per la fatturazione di un prodotto o servizio. Riguardo a quest'ultimo punto, è bene ricordare che le società non devono, ad esempio, chiedere ai "clienti" il consenso per l'uso dei loro dati quando rilasciano carte di fedeltà (come quelle dei supermercati o dei benzinai) al solo fine di offrire sconti, premi, bonus, servizi accessori, facilitazioni di pagamento; in questo caso, infatti, il trattamento di dati è necessario per eseguire gli obblighi derivanti dal contratto di fidelizzazione sottoscritto. È invece richiesto uno specifico consenso per usare gli stessi dati per altri fini come la profilazione, lo studio dei comportamenti e delle scelte d'acquisto, il marketing in generale. I consumatori hanno il diritto di non dare il consenso all'uso dei dati per tali scopi, senza per questo dover rinunciare alla tessera di fidelizzazione.
Le imprese sono invece esonerate dall'obbligo di acquisizione del consenso per le attività promozionali e di marketing rivolte ai propri clienti effettuate tramite la posta elettronica o la posta cartacea. In particolare, una società non deve richiedere il consenso per inviare comunicazioni promozionali che riguardino prodotti e servizi alla persona che ha già acquistato, dallo stesso titolare, beni analoghi (è il cosiddetto "soft spam").
Naturalmente il cliente deve essere adeguatamente informato anche riguardo alla possibilità di opporsi in qualunque momento all'uso dei propri dati, in maniera agevole e gratuita, anche a voce o con l'invio di una e-mail, ottenendo un tempestivo riscontro dall'impresa che confermi l'interruzione delle comunicazioni commerciali.
Si possono trattare senza consenso anche i dati relativi allo svolgimento di attività economiche - naturalmente

nel rispetto della vigente normativa in materia di segreto aziendale e industriale - compiute dall'interessato (ad esempio i dati relativi allo stato di insolvenza o alla correttezza commerciale di una impresa individuale).
Non è necessario il consenso degli interessati neppure per utilizzare i dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque. Il fatto che un dato sia conoscibile da chiunque non significa, però, che possa essere utilizzato per qualunque attività.
In particolare, va rispettato rigorosamente il vincolo di finalità: i dati disponibili al pubblico possono essere utilizzati solo se il trattamento svolto (come l'invio di comunicazioni informative) risulta strettamente attinente alla specifica attività svolta dall'interessato e che è posta alla base della pubblicazione di quei medesimi dati. I dati del PRA (Pubblico Registro Automobilistico) si possono usare senza consenso per finalità attinenti la sicurezza stradale (ad esempio

per ricordare l'obbligo di revisione periodica dell'autoveicolo) ma non per l'invio di pubblicità come quelle su pezzi di ricambio e accessori.
Al fine di evitare inutili adempimenti, è inoltre previsto che non sia richiesto il consenso per alcune attività svolte all'interno di gruppi di imprese come nel caso in cui sia necessario comunicare i dati per finalità meramente amministrativo-contabili (ad esempio quelli che possono riguardare clienti, fornitori e dipendenti).
Si segnala infine, tra i numerosi casi, che non è necessario ottenere il consenso dell'interessato anche quando il trattamento dei dati è necessario ai fini dello svolgimento di investigazioni difensive o comunque per far valere un diritto in sede giudiziaria.

Consenso e dati sensibili

È necessario ricordare che i dati sensibili, come le informazioni sulla salute di una persona, necessitano di tutele rafforzate. Per poterli utilizzare, l'impresa deve prima ottenere il **consenso scritto** della persona interessata e l'**autorizzazione** del Garante. Anche in questo caso, per agevolare la normale attività imprenditoriale, l'Autorità fin dalle sue origini ha semplificato al massimo le procedure e ha adottato alcune **autorizzazioni generali** che valgono per intere categorie di soggetti o per determinate tipologie di trattamento, al fine di definire le regole per gli utilizzi più comuni ed evitare la richiesta di autorizzazioni *ad hoc*. Ne rappresenta un esempio l'autorizzazione generale per il trattamento dei dati sensibili o giudiziari nell'ambito del rapporto di lavoro o per il trattamento effettuato da liberi professionisti o da organismi di tipo associativo o dalle fondazioni.
In specifici casi, al fine di facilitare l'uso dei dati, non è previsto neppure il consenso dell'interessato, come per l'adempimento degli specifici obblighi e compiti previsti per la gestione del rapporto di lavoro.

Curriculum & Co.

4

Durante tutte le fasi del processo di selezione del personale vi è un'intensa attività di trattamento di dati personali dei possibili candidati. Il rispetto della privacy, però, non pone limiti all'incontro della domanda di lavoro con la disponibilità dei posti offerti dalle imprese, finalità che va sempre incoraggiata.
A tal proposito, il Garante ricorda che, in base alle disposizioni del Codice della privacy, è assolutamente superfluo richiedere al candidato il consenso al trattamento dei dati personali contenuti nel curriculum, per finalità di selezione del personale, a meno che non abbiano natura sensibile (come l'appartenenza a categorie protette) o non siano destinati alla comunicazione a terzi.
L'impresa che avvia una selezione del personale deve però fornire al candidato, a voce o per iscritto, prima di acquisire il suo cv, l'informativa sul trattamento dei dati personali.
Sono state recentemente introdotte nuove norme che agevolano invece le procedure che l'impresa deve adottare quando è l'interessato stesso a far pervenire di sua iniziativa il curriculum (**autocandidatura**). In questo specifico caso, l'azienda che riceve i curriculum inviati spontaneamente non ha l'obbligo di offrire l'informativa o di chiedere al candidato il consenso per il trattamento dei dati personali (inclusi quelli sensibili) contenuti nella documentazione pervenuta.
Solo nel momento in cui l'azienda decida di prendere in considerazione il curriculum e di contattare il candidato, dovrà fornire all'interessato, anche a voce, una informativa breve con l'indicazione delle finalità e modalità del trattamento dei dati, i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati, e l'ambito di diffusione dei dati medesimi, nonché gli estremi identificativi del titolare e di almeno un responsabile, se designato.

5 Trattamenti “a rischio”

Al fine di garantire maggiore trasparenza e tutele nel caso in cui vengano effettuati trattamenti di dati di particolare delicatezza e di potenziale pericolosità, il Codice della privacy ha previsto che, in casi specifici, le imprese comunichino preventivamente al Garante informazioni generali sull’attività di raccolta e di utilizzazione dei dati personali. Una volta effettuata la “notifica” del trattamento, non è necessario che l’azienda invii altre comunicazioni al Garante, a meno che il trattamento non sia modificato o interrotto. Tutte le notificazioni telematiche pervenute sono inserite in un **registro pubblico** consultabile da chiunque sul sito web dell’Autorità.
La **notificazione** è appunto una comunicazione telematica obbligatoria quando si effettuano determinati tipi di trattamento. Vanno notificati fra gli altri i trattamenti di dati genetici, biometrici o di dati che indicano la posizione geografica di persone o di oggetti a loro riferibili (come i sistemi di geolocalizzazione) acquisiti, ad esempio, con rilevamenti radio; i trattamenti di dati per le attività di profilazione, e così pure la raccolta di informazioni in apposite banche dati relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni (vi rientrano ad esempio gli archivi dei cosiddetti sistemi di informazioni creditizie) e a comportamenti illeciti o fraudolenti. A tal proposito, il Garante ricorda che non devono però essere notificati i trattamenti dei dati relativi agli inadempimenti contrattuali dei propri clienti conservati da ciascuna impresa.
Anche nel caso della notificazione il Garante, per facilitare le attività standard dei vari settori, ha introdotto **esoneri specifici** che possono riguardare figure professionali o intere categorie di professionisti come avvocati, medici di base e pediatri, oppure organismi di mediazione, rispetto a determinati profili della loro attività.

Tecnologie per l'impresa

6

Nell'ambito dell'attività imprenditoriale si perseguono numerosi e variegati interessi, come quello di migliorare le capacità di analisi del mercato, di garantire maggiore sicurezza sul lavoro, di difendere i propri beni e investimenti infrastrutturali da accessi non autorizzati, danneggiamenti e rapine, oppure di ridurre comportamenti fraudolenti o non in linea con le direttive aziendali. Questi legittimi interessi possono essere perseguiti con molteplici soluzioni tecnologiche e organizzative, alcune delle quali, se comportano un trattamento di dati personali, possono però confliggere con la dignità e la riservatezza delle persone coinvolte. In questi casi è previsto l'intervento del Garante per valutare e "bilanciare" i diritti e gli interessi esistenti.

Controllo sul lavoro

L'imprenditore deve ponderare con attenzione quali strumenti adottare al fine di evitare trattamenti di dati non necessari che, tra l'altro, possono risultare eccessivi o anche discriminatori. È lecito, ad esempio, installare un sistema di videosorveglianza per esigenze organizzative e produttive, per consentire, ad esempio, di intervenire immediatamente nel caso in cui si verifichino situazioni di rischio (come negli ambienti dove si effettuano lavorazioni pericolose).

Ma se tale raccolta di immagini può consentire anche il **controllo a distanza** e la verifica dell'attività dei lavoratori, occorre tenere in considerazione non solo le norme previste dal Codice della privacy, ma anche quelle indicate nello **Statuto dei lavoratori** (tenendo presente che l'installazione di tecnologie per l'esclusiva finalità di controllo a distanza dei lavoratori è comunque vietata). Pari cautele vanno adottate, ad esempio, anche quando si utilizzano software che, al fine di migliorare le prestazioni della rete internet aziendale, potrebbero però consentire il monitoraggio della navigazione o della posta elettronica dei dipendenti.
Occorre definire bene anche l'utilizzo di tecnologie che consentono la precisa localizzazione del lavoratore come, ad esempio, il Gps dell'autoveicolo o dello smartphone in dotazione, o l'Rfid (Identificazione a radio frequenza) del documento di riconoscimento. Ciò non significa che non si possa ricorrere alla geolocalizzazione, ma che devono essere valutate tutte le circostanze del caso e la proporzionalità del suo utilizzo. Anche in questi casi il Garante è intervenuto per semplificare l'attività aziendale, facilitando l'attività di controllo della flotta aziendale senza per questo limitare i diritti dei lavoratori.
Altre volte lo strumento adottato non consente necessariamente il monitoraggio dell'attività del lavoratore, ma si dimostra comunque sproporzionato rispetto alle finalità dichiarate. Succede spesso quando si decide di usare dati biometrici (come il riconoscimento dell'iride o il codice numerico riferibile all'impronta digitale) per **controllare gli accessi** in una determinata area. Tale misura è giustificata solo in situazioni di particolare rischio.

Verifica preliminare

La normativa sulla privacy, al fine di evitare possibili gravi pregiudizi alle persone interessate e successivi problemi alle imprese, prevede che il Garante debba essere contattato

preventivamente, chiedendo una **verifica preliminare**, nel caso in cui la società intenda avviare un trattamento di dati personali (diversi da quelli sensibili e giudiziari) che possa presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato. Tale situazione può verificarsi sia per la natura dei dati o per le modalità del trattamento o per gli effetti che il trattamento stesso può determinare. È necessario richiedere una verifica preliminare, ad esempio, quando si intendono attivare sistemi di videosorveglianza "intelligente" - come quelli in grado di rilevare automaticamente comportamenti o eventi anomali - oppure quelli dotati di un software che consenta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (ad es. la morfologia del volto) con dati biometrici, o sulla base del confronto dell'immagine con una campionatura di soggetti precostituita alla rilevazione dell'immagine. La verifica preliminare è richiesta anche quando, per particolari esigenze, si vogliano allungare i tempi di conservazione delle immagini registrate oltre il termine massimo di sette giorni, a meno che questa necessità non derivi da una specifica richiesta dell'autorità giudiziaria o di una forza di polizia per un'attività investigativa in corso. La normativa, quindi, non vieta in assoluto l'adozione di misure tecnologiche a tutela delle attività aziendali, ma cerca un **bilanciamento** con altri diritti fondamentali della persona. L'eventuale autorizzazione concessa dall'Autorità, a conclusione della verifica preliminare, può essere inoltre vincolata da precise condizioni come, ad esempio, quella che impone alle banche di garantire modalità di accesso alternativo ai clienti che non desiderano lasciare la propria impronta digitale (dato biometrico) per entrare nelle agenzie o per accedere ai locali dove sono custodite le cassette di sicurezza.

7 Difesa del patrimonio dati

Nessuna società desidera che la lista dei propri clienti, i propri contatti, i dati personali dei propri impiegati e dirigenti, le fatture, la posta interna o persino i propri segreti industriali (piani di sviluppo, dettagli di brevetti...) finiscano nelle mani della concorrenza o di qualche malfattore. I dati raccolti da un'impresa rappresentano infatti un *asset* fondamentale per il suo successo sul mercato.
Questa incomprimibile necessità aziendale si trasforma in un obbligo di legge quando ad essere raccolti, conservati o trattati in qualunque modalità sono dati personali.
Devono quindi essere adottate idonee e preventive **misure di sicurezza**, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Bastano talvolta poche azioni per mettere al sicuro questi beni tra i più preziosi che l'azienda detiene ma che si riferiscono ad altre persone.
Se sono conservati in formato cartaceo potrebbe essere sufficiente mettere un lucchetto all'armadio o alla stanza dove sono archiviati documenti e fascicoli, nonché definire le regole a cui devono sottostare le persone che hanno la "chiave" per accedervi e per trattarli.
Se invece sono in formato digitale, come quelli trattati attraverso computer, *tablet* o *smartphone*, è necessario applicare misure più complesse e adeguate al tipo di rischio.

Misure minime

Al di là di prescrizioni *ad hoc* per settori particolari, il Codice prevede che per il trattamento dei dati è necessario che i titolari adottino **misure minime** di sicurezza che garantiscano, ad esempio, in caso di trattamento elettronico, la verifica e la convalida dell'identità di chi accede al sistema (identificativi personalizzati, password sicure...), l'adozione di un apposito

sistema di autorizzazione che consenta solo specifiche attività predefinite, l'utilizzo di strumenti (come antivirus aggiornati e altri software e sistemi di protezione) per impedire accessi illeciti o abusivi che mettano a rischio l'integrità e la confidenzialità del dato personale.

Bisogna poi essere pronti a gestire situazioni di crisi, ad esempio predisponendo "copie di *backup*", in modo da poter rendere nuovamente disponibili dati e sistemi. Occorre anche definire misure di protezione particolari per i dati sensibili, magari adottando tecniche crittografiche

che non li rendano immediatamente leggibili in caso di accessi illeciti.
Il settore informatico è in rapida e costante evoluzione, è quindi importante, per la sicurezza dell'azienda e per la protezione dei dati personali, che il personale addetto a queste attività riceva un'adeguata formazione e che le misure adottate, per non perdere di efficacia, siano aggiornate nel tempo.
È venuto recentemente meno, invece, l'obbligo di predisporre un "documento programmatico sulla sicurezza" che elenchi le misure adottate. Le imprese potranno comunque trarre beneficio da un monitoraggio frequente della propria privacy policy e delle misure adottate per proteggere i dati, mantenendo così sotto controllo la situazione.
Per facilitare la normale attività svolta presso liberi professionisti, artigiani e piccole e medie imprese, il Garante ha previsto che le misure minime possano essere applicate in forma semplificata nel caso in cui i dati personali siano trattati unicamente per correnti finalità amministrative e contabili. Sono state semplificate anche le misure di sicurezza dei soggetti che trattano solamente dati sensibili connessi alla gestione operativa del rapporto di lavoro (malattia, partecipazione ad attività sindacali).

Misure idonee

A volte, in base alla complessità tecnologica dell'azienda e al livello di rischio a cui si è sottoposti, l'adozione delle misure minime di sicurezza potrebbe risultare non sufficiente.
L'imprenditore (il titolare e i responsabili del trattamento), nel caso in cui a seguito di violazioni dei dati sia chiamato in causa per un'azione risarcitoria in sede civile, dovrà affrontare le difficoltà derivanti dall'inversione dell'onere della prova, e dovrà essere in grado di dimostrare di aver adottato tutte le **misure idonee**, in base allo stato dell'arte, a ridurre - per quanto possibile - i rischi connessi al non corretto utilizzo dei dati.

In ogni caso, l'Autorità può indicare anche di propria iniziativa le **misure opportune o necessarie** per far sì che un determinato tipo di trattamento sia conforme alla normativa sulla privacy. Per rendere tracciabili certe operazioni, come quelle effettuate su dati bancari o informazioni fiscali, può ad esempio essere previsto l'obbligo di adottare specifici sistemi di monitoraggio con *alert* automatici che segnalino intrusioni, accessi o comportamenti anomali o tali da configurare eventuali trattamenti illeciti.

Cloud Computing

Deve essere prestata particolare attenzione alla modalità con cui si adottano innovazioni tecnologiche, come quelle offerte dal *cloud computing*, affinché le eventuali opportunità di efficienza e risparmio non si trasformino in un rischio per la sicurezza dei dati dell'impresa. L'Autorità, proprio per facilitare una scelta consapevole delle aziende, ha pubblicato sul proprio sito Internet un'apposita guida sull'uso di queste nuove tecnologie.

Rifiuti tecnologici

Il Garante ha anche segnalato alle imprese i rischi, spesso sottovalutati, che possono emergere da un non adeguato smaltimento di apparecchiature elettriche ed elettroniche come hard disk, chiavi di memoria, dischetti, vecchi telefoni cellulari, *tablet* o *smartphone*. Questi apparati possono infatti contenere grandi quantità di dati personali che, se non opportunamente cancellati prima dello smaltimento, possono essere poi recuperati da malintenzionati o da persone che comunque non hanno diritto di accedervi. L'Autorità ha quindi fornito consigli e indicato le opportune misure tecniche che devono essere adottate per la memorizzazione (come l'utilizzo di tecniche di cifratura) o la cancellazione sicura (ad esempio con l'uso di appositi software o con la distruzione fisica dei supporti) dei dati riservati di un'impresa.

8 Controllo del “controllore informatico”

All’interno delle grandi imprese, in genere, esiste una figura particolare che si occupa della gestione dei sistemi informatici e della sicurezza: l’**amministratore di sistema**. Proprio per la peculiarità delle sue funzioni, questo professionista può avere accesso ai dati più riservati di un’azienda. Per questo motivo il Garante ha prescritto che anche il suo operato sia trasparente e posto sotto il controllo del titolare del trattamento. Occorre innanzitutto valutare con attenzione l’esperienza, la capacità, e l’affidabilità delle persone chiamate a ricoprire tale ruolo, conservando poi un elenco con i loro estremi identificativi e con l’indicazione delle funzioni ad essi attribuite.

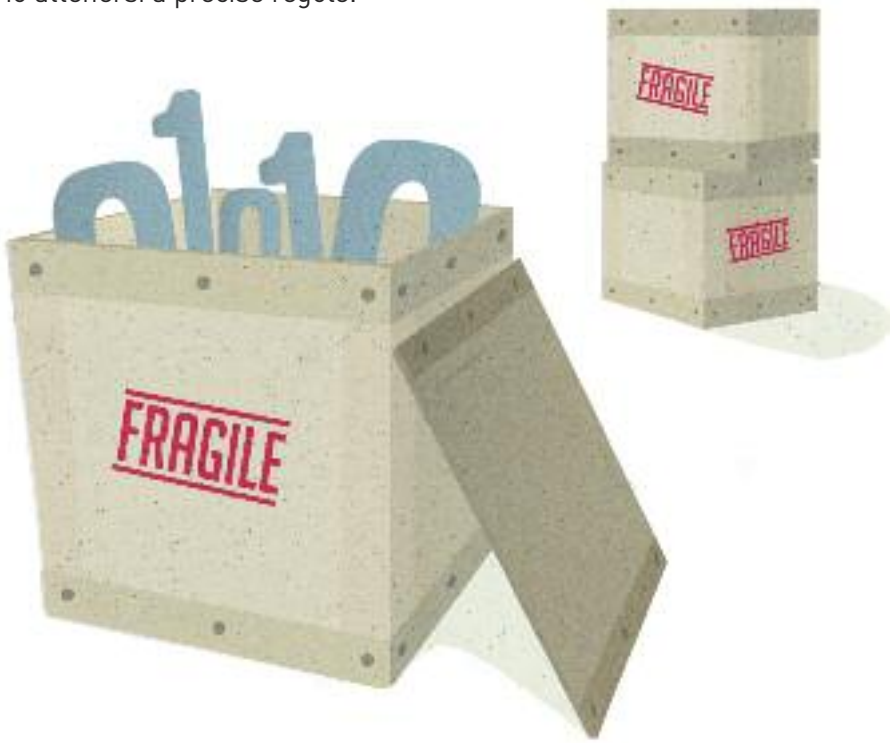
Devono essere utilizzati sistemi di controllo (presenti in tutti i moderni sistemi operativi oggi in uso) che consentano la tracciabilità degli accessi effettuati dagli amministratori di sistema agli archivi elettronici e ai sistemi di elaborazione, e la registrazione dei relativi dati per un tempo non inferiore ai sei mesi (a questo scopo sono disponibili anche gratuitamente appositi strumenti software). Il titolare del trattamento dovrà poi provvedere a una verifica, con cadenza almeno annuale, sulla rispondenza dell’operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.
Queste misure, naturalmente, non si applicano a quei soggetti (ad esempio professionisti, piccole imprese, associazioni) che sono dotati di sistemi informatici di modesta e limitata entità e che, quindi, non fanno ricorso a una figura professionale specificamente dedicata all’amministrazione dei sistemi informatici.

L’ “export” dei dati

9

Non tutti i beni possono essere portati all’estero. Esistono ad esempio limiti al trasferimento di valuta, o di prodotti materiali e immateriali, oppure vincoli dettati da ragioni di sicurezza e di mantenimento della qualità del prodotto. Anche per poter “esportare” dati personali è necessario attenersi a precise regole.

La normativa comunitaria prevede infatti che i dati personali possono circolare liberamente entro l’Unione europea. Per trasferire dati al di fuori dell’Unione europea devono invece essere garantiti **standard di protezione adeguati a quelli europei**:
in caso contrario è vietato trasferire dati personali.



Per semplificare l'attività di ricognizione dell'imprenditore che ha necessità di trasferire i dati, il Garante pubblica sul proprio sito internet un **elenco aggiornato degli Stati "terzi"**(cioè non appartenenti all'Unione europea o allo Spazio Economico Europeo) che sono già ritenuti affidabili a livello europeo e per i quali non è necessario alcun "passaporto" per l'esportazione.

Trasferimenti di dati verso Paesi "non certificati"

Se il paese scelto non è in questa lista, l'eventuale trasferimento dei dati può essere consentito sulla base di **altre garanzie adeguate**. Per quanto riguarda gli Stati Uniti, si può controllare se i dati sono trasferiti ad imprese presenti sul territorio americano che aderiscono ad un accordo bilaterale UE-USA detto *Safe Harbor* (letteralmente "porto sicuro"), il quale definisce regole sicure e condivise per il trasferimento dei dati personali. Nel caso di imprese multinazionali, quindi operanti in più Paesi anche su diversi continenti, che devono trasferire dati "infragruppo", cioè all'interno della propria complessa struttura societaria (ad esempio tra imprese collegate o controllate, comunque facenti parte del gruppo), si può verificare se sono state adottate adeguate norme vincolanti d'impresa (*Binding Corporate Rules*) che devono essere autorizzate dalle autorità europee di protezione dati, attraverso una specifica procedura che coinvolge anche il Garante italiano.
In tutti gli altri casi, valgono le **eccezioni** al divieto di trasferire dati in Paesi terzi: è consentito, ad esempio, il trasferimento se vi è l'apposito consenso dell'interessato (consenso scritto nel caso in cui si tratti di dati sensibili), oppure quando il trasferimento risulta necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato.

Verso una “customer care dei dati” 10

Un’impresa competitiva, che desidera sviluppare buone relazioni con la clientela e con le controparti, risponde con velocità e completezza alle richieste che giungono al *customer care* o agli altri uffici competenti. Più in generale, le buone prassi che si sono delineate in questo decalogo possono contribuire a rafforzare la capacità dell’impresa nel gestire al meglio i dati personali che le sono affidati, e al tempo stesso la fiducia dei clienti e del pubblico nell’affidabilità e modernità della struttura aziendale. Il patrimonio informativo di un’azienda è un valore da tutelare e promuovere alla stregua di ogni altro *asset*, e può trasformarsi in una risorsa competitiva e di immagine.

Diritti della persona interessata

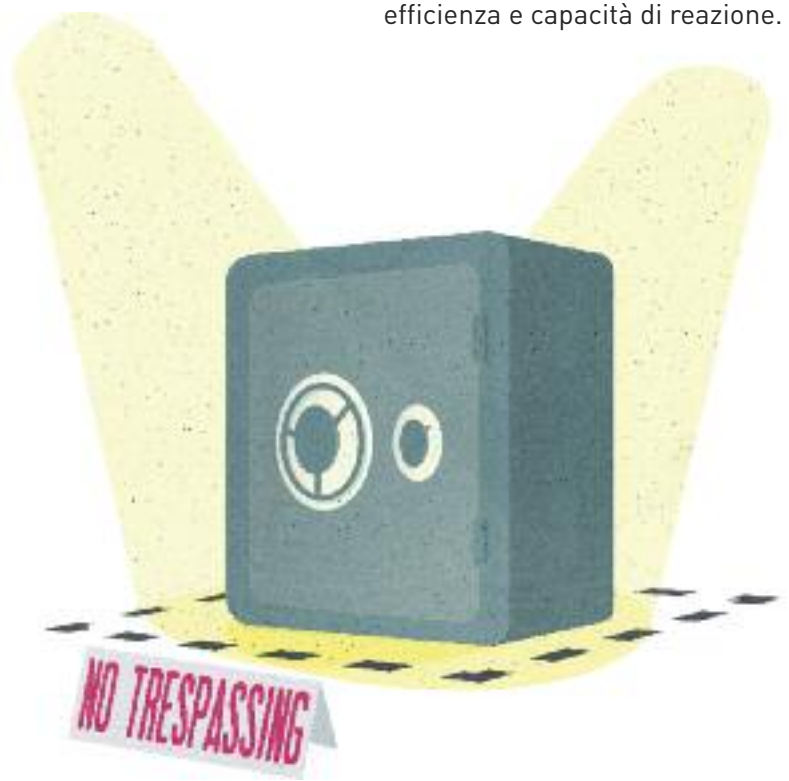
In tale ambito, è opportuno che anche le richieste di informazione in merito al trattamento effettuato con i dati personali vengano gestite adeguatamente. La normativa sulla privacy, tra l’altro, garantisce alla

persona interessata - ad esempio dipendente, cliente o utente - **specifici diritti** come quello di conoscere quali siano i dati che lo riguardano in possesso dell'impresa e per quale motivo siano stati raccolti e come siano elaborati. Può richiedere l'estrapolazione e la messa a disposizione in modo intelligibile dei dati personali che lo riguardano e, se ne ha interesse, il loro aggiornamento, la rettifica o l'integrazione. In caso di violazione di legge, può anche esigere il blocco, la cancellazione o la trasformazione in forma anonima di queste informazioni.
Tra l'altro si rammenta che, in linea generale, un dato personale non deve essere conservato per sempre, ma solo fin quando è necessario per lo scopo per il quale i dati sono stati raccolti. Qualora non sia indicato per legge un preciso termine di conservazione, occorre comunque prevederlo.
Una risposta puntuale e completa da parte della società è sempre un indicatore positivo di efficienza e trasparenza, e contribuisce a rafforzare la fiducia dei clienti/utenti oltre ad evitare un intervento del Garante da cui possano derivare provvedimenti inibitori, prescrittivi o anche sanzionatori per il mancato rispetto dei diritti dell'interessato.

Distruzione o perdita di dati personali

Le imprese dovrebbero reagire con prontezza e trasparenza ogni volta in cui dovessero accorgersi di violazioni dei dati personali trattati. In questi casi, al di là delle opportune valutazioni in termini di responsabilità civile e penale, sarebbe sempre opportuno **avvisare gli interessati** del problema riscontrato, anche per consentire loro di adottare misure che limitino i possibili **pregiudizi alla persona** che possono derivare, ad esempio, da un furto di identità o il danno alla reputazione che può discendere dall'utilizzo di dati inesatti o non aggiornati.
Alcuni dei settori più esposti in tal senso sono quello bancario, della

sanità e delle telecomunicazioni.
Per garantire maggiori tutele ai consumatori, una recente disposizione europea, ora adottata anche in Italia, impone alle società telefoniche e ai fornitori di servizi di accesso a Internet un vero e proprio obbligo di comunicare al Garante della privacy, e in certi casi anche agli utenti stessi, eventuali gravi "violazioni di dati personali" subite dalle loro banche dati (le cosiddette *data breaches*) che dovessero comportare perdita, distruzione o diffusione indebita di dati. In caso di attacchi informatici o di eventi avversi, quali incendi o altre calamità, l'impresa avrà così non solo l'obbligo ma anche l'opportunità di dimostrare la propria efficienza e capacità di reazione.



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Antonello Soro, Presidente
Augusta Iannini, Vice Presidente
Giovanna Bianchi Clerici, Componente
Licia Califano, Componente

Giuseppe Busia, Segretario generale

Garante per la protezione
dei dati personali
Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785

Per informazioni presso l'Autorità:
Ufficio per le relazioni con il pubblico
Lunedì - Venerdì ore 10.00 - 13.00
tel. 06 696772917/9
e-mail: urp@garanteprivacy.it
pec: urp@pec.gpdp.it

A cura del Servizio relazioni
con i mezzi di informazione

Maggio 2013

www.garanteprivacy.it

Stampa: IAG Mengarelli
ill: M. Polverini
VERTIGO DESIGN