Dati bancari o fiscali, richiedono particolari protezioni, alert automatici che segnalino intrusioni, anomalie, comportamenti illeciti. L'impresa, se chiamata in tribunale per un'azione risarcitoria in sede civile, deve dimostrare di averle adottate.

Esportazione di dati
I dati personali possono circolare liberamente all'interno della **UE**.

Quanto agli **Stati Terzi**, il Garante pubblica sul sito l'elenco aggiornato di quelli ritenuti affidabili.

Per gli **Stati Uniti**, si può controllare se i dati confluiscono in imprese che appartengono a un accordo bilaterale Ue-Usa, come il *Safe Harbour*.

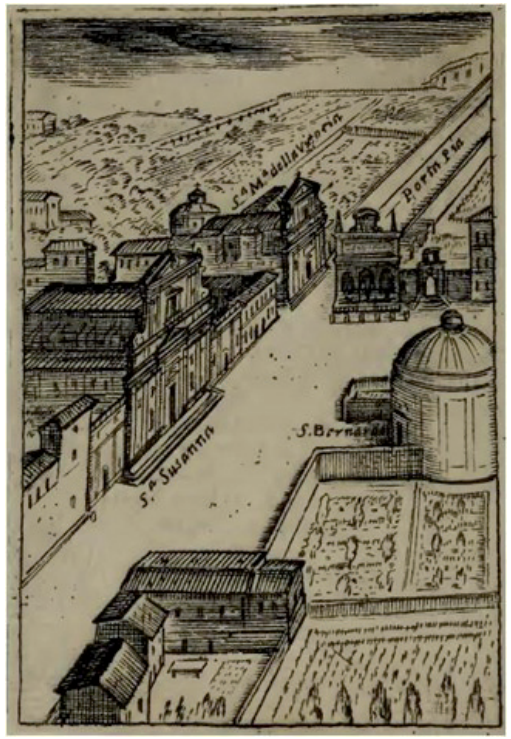
Nel caso di **multinazionali** si può controllare che abbiano policy vincolanti (binding corporate rules), che comunque devono essere controllate dalle autorità europee. In tutti gli altri casi di **paesi terzi**, sono necessarie pratiche di controllo.

Customer care

L'interessato può sempre informarsi sui propri dati, come sono stati raccolti ed elaborati, può richierne l'aggiornamento, la cancellazione, la correzione, la trasformazione in forma anonima.

Buone pratiche: conservare i dati solo per il tempo necessario alle finalità a cui servono, avvisare gli interessati quando si verificano intrusioni o violazioni (obbligatorio per società di TLC e fornitori di servizi internet).

Avv. Andrea Colletti
Avvocato presso le giurisdizioni superiori
Socio Agathemis Studio Legale Associato



VIA XX SETTEMBRE, 118 - 00187 ROMA
TEL. +39 06.47825609 - FAX +39 06.4789630396
info@agathemis-studiolegaleassociato.it
www.agathemis-studiolegaleassociato.it

IMPRESA ED ADEMPIMENTI PRIVACY
LE LINEE GUIDA DEL GARANTE

Agathemis®
Studio Legale Associato

Dal punto di vista dell'azienda che opera nell'ambito delle nuove frontiere della tecnologia e del marketing, un utile richiamo di normativa e di pratiche adeguate da porre in essere è stato pensato dal Garante per la protezione dei dati personali
Il "vademecum", dal titolo emblematico "La privacy dalla parte dell'impresa", offre alle PMI (Piccole Medie Imprese) una serie di pratiche aziendali per migliorare il business ed agire in conformità normativa nella gestione dei dati di clienti e dipendenti, alla luce delle nuove tecnologie (biometria, geolocalizzazione) ed attività di marketing.

E' bene ricordare che, in tema di adempimenti a carico dell'impresa, il D.L. n. 5/2012 (cosiddetto Decreto Semplificazioni) ha abrogato, a decorrere dal 10.02.2012, l'obbligo di redigere il Documento Programmatico per la Sicurezza dei dati trattati (DPS), ossia il documento che riassumeva tutte le procedure e misure di sicurezza predisposte dal Titolare del trattamento.
Con la nuova semplificazione è quindi venuto meno anche l'obbligo del Titolare di riportare, all'interno della relazione accompagnatoria del bilancio d'esercizio, l'annotazione relativa alla redazione o all'aggiornamento di tale documento.

Dopo l'abolizione del DPS, restano comunque vigenti le previsioni contenute negli art. 33 e ss. del D.Lgs. 196/2003 e pertanto le aziende dovranno continuare a disciplinare il trattamento dei dati nel rispetto delle misure minime di sicurezza.

Quali sono i dati da tutelare
- Personali: anagrafici, indirizzi fisici o email, immagini fotografiche, codice fiscale, numero di telefono, targa automobilistica.
- Sensibili: religione, adesione a partiti o sindacati, salute, vita sessuale.
- Giudiziari: casellario giudiziale, posizione di indagato o imputato in procedimenti penali.
- Biometrici (inquadramento di una persona sulla base di una o più caratteristiche biologiche e/o comportamentali).

I titoli di responsabilità nel trattamento dei dati
L'azienda o l'imprenditore individuale è il Titolare del trattamento, che può nominare con atto scritto un responsabile interno o esterno all'impresa, precisandone i compiti.

Gli Incaricati sono invece le persone che materialmente accedono e gestiscono i dati, designati per iscritto o facenti parte dell'unità/ufficio di riferimento del responsabile.
L'Amministratore di sistema è invece la figura specificamente dedicata alla gestione dei sistemi informatici e della sicurezza, ha accesso (tracciabile) a dati molto riservati, è sotto il diretto controllo del titolare del trattamento.

Informativa e consenso
L'impresa deve informare dipendenti e clienti in modo completo e chiaro, specificando:
- le finalità del trattamento dei dati,
- a chi possono essere comunicati i dati o chi può venirne a conoscenza,
- il nome del responsabile del trattamento, se persona diversa dal titolare.

L'utilizzo dei dati a fini di marketing non può mai essere obbligatorio, ponendolo come condizione per accedere a contenuti informativi o servizi.
Oltre a informare l'interessato, va chiesto il consenso dello stesso per l'utilizzo dei dati, consenso liberamente espresso in forma scritta e differenziato a seconda del trattamento, fatta evidenza della differente natura dei dati.
Soft spam: un'azienda può inviare messaggi promozionali via mail o per posta ma il cliente può opporsi, inibendo l'ulteriore invio, anche oralmente.

Quanto alla particolare categoria dei dati sensibili e biometrici, nonché per i dati relativi a rischio di solvibilità economica, situazione patrimoniale, informazioni creditizie, comportamenti illeciti o fraudolenti, non è sufficiente il consenso dell'interessato, ma occorre apposita **preventiva autorizzazione del Garante.**

Curriculum Vitae: chiedere al candidato che invia un curriculum il consenso al trattamento dei dati è superfluo, a meno che i dati siano destinati a comunicazioni a terzi. L'impresa è però tenuta a fornire l'informativa sul trattamento dei dati quando avvia un selezione di personale.

Tecnologie
Per alcune **tecnologie** (monitoraggio della posta o della navigazione del dipendente, flotta aziendale con localizzazione Gps, geolocalizzazione, smartphone) ci sono regole generali: cautela e informativa con finalità dichiarate, che non possono essere sproporzionate. Per avvisare che un veicolo aziendale è sottoposto a **geolocalizzazione**, per esempio, si può applicare apposito adesivo sulla vettura.

Per i sistemi di **videosorveglianza** dei dipendenti vanno rispettate le norme dello Statuto dei Lavoratori (vietato il controllo a distanza fine a se stesso, deve essere legittimato da esigenze di sicurezza, o di prevenzione rischi). Le immagini possono essere conservate per massimo **sette giorni**. Per esigenze particolare serve la preventiva verifica del Garante, che può dare un via libera condizionato.

Stessa procedura (verifica preliminare e autorizzazione del Garante) per i **dati biometrici:** la misura deve comunque essere giustificata da condizioni di particolare rischio.

Cloud Computing: anche per quest'aspetto il Garante ha predisposto un'apposita guida che evidenzia buone pratiche:

- Attenta valutazione del **provider** a cui affidarsi
- Privilegio dei servizi che favoriscono la **portabilità dei dati** (per poter eventualmente passare da un sistema all'altro)
- Disponibilità dei dati in caso di necessità,
- Conoscenza di dove risiederanno concretamente i dati (dove sono i **server**),
- Tempi e modalità di **conservazione**,
- Clausole contrattuali sulla perdita o violazione dei dati,
- Sicurezza: quando si smaltiscono hard disk, apparecchiature, telefonini, cancellare tutti i dati che contengono. Opportuna l'adozione di specifici software.

Difesa dei dati
Per ridurre il rischio di distruzione, perdita e accessi non autorizzati, ecco le **misure minime** da adottare:

- Convalida dell'indentità (password),
- Sistema che consenta solo determinate azioni predefinite,
- **Antivirus** e software di sicurezza,
- Copie di **backup**,
- Crittografia per i dati sensibili.

Non è più necessario - come detto - il *"documento programmatico sulla sicurezza*" che elenchi le misure adottate.