Cristina Vicarelli
Avvocato

Checklist sulla privacy

Mi sono accorta che alcuni utenti approdano sul mio blog cercando una checklist sulla privacy, pertanto ho deciso di fornirne indicazioni a chi fosse interessato a utilizzare uno strumento sintetico di controllo per avere una prima immediata percezione della propria compliance alle regole sulla protezione dei dati personali e degli adempimenti che fossero eventualmente da implementare. La prima annotazione che ritengo di dover fornire riguarda la nostra Autorità Garante. Nel lontano 2007, infatti, sul sito dell'Autorità è stata pubblicata la "Guida pratica e misure di semplificazione per le piccole e medie imprese". Il provvedimento offre un'utile check list che per comodità riporto (aggiornandola al presente quadro normativo) anche se andrebbe letta insieme al provvedimento, dato che alcuni aspetti potrebbero non essere di immediata percezione, se non si ha familiarità con il linguaggio tecnico:

Quesito	**SÌ**	**NO**
1. I soggetti che effettuano il trattamento		
È stata effettuata una valutazione circa le operazioni di trattamento di dati personali, anche sensibili, effettuate dall'impresa?		
I dati trattati sono pertinenti e non eccedenti rispetto alle legittime finalità del trattamento, oltre che esatti e aggiornati?		
Le persone fisiche che all'interno dell'impresa trattano dati personali sono state designate tutte quali "incaricate del trattamento"?		
Sono state fornite a tutti gli "incaricati del trattamento" istruzioni scritte circa i propri compiti? (NDR si veda anche la possibilità di impartire istruzioni orali nel provvedimento di semplificazione del 2008)		
Se all'interno dell'impresa sono stati individuati soggetti che hanno ambiti di autonomia nel trattamento dei dati personali, sono stati designati per iscritto "responsabili del trattamento"?		
Se fuori dell'impresa enti o persone fisiche trattano dati personali nel suo interesse, obbligati a seguirne le istruzioni (come accade per i casi di outsourcing), sono stati designati per iscritto quali "responsabili del trattamento"?		

Quesito	SÌ	NO
2. La notificazione del trattamento		
Si è verificato, prima di intraprendere operazioni di trattamento, se l'impresa effettua i trattamenti da notificare al Garante?		
Se sono intervenute modificazioni relativamente ai trattamenti già eventualmente notificati, è stato curato il loro aggiornamento in una nuova notificazione?		
Se cessano i trattamenti, ciò ha formato oggetto di specifica notificazione?		
3. L'informativa		
È stata fornita l'informativa agli interessati in caso di dati raccolti presso di essi?		
È stata fornita l'informativa agli interessati in caso di dati raccolti presso soggetti diversi dagli interessati stessi?		
4. Il consenso dell'interessato		
Il trattamento dei dati personali viene effettuato in presenza di uno dei presupposti di liceità indicati all'art. 24 del Codice?		
Se non ricorre uno dei presupposti di liceità indicati all'art. 24 del Codice, è stato raccolto il consenso dell'interessato?		
Se sono trattati dati sensibili è stato raccolto il consenso scritto degli interessati?		
Se sono trattati dati sensibili, è stato verificato se il trattamento rientra tra quelli già autorizzati dal Garante con le autorizzazioni generali?		
Se il trattamento di dati sensibili non rientra tra quelli previsti dalle autorizzazioni generali, è stata richiesta al Garante un'autorizzazione ad hoc?		
5. La sicurezza dei dati		
Sono state adottate idonee misure di sicurezza per proteggere i dati personali?		
Sono state adottate le misure minime di sicurezza previste per proteggere i dati personali? (NDR anche qui si veda il provvedimento di semplificazione linkato al punto 1)		
Omissis (quesiti- riferiti al DPS ormai abrogato)		

Quesito	SÌ	NO
6. Il trasferimento dei dati in paesi terzi		
Se i dati personali trattati dall'impresa sono soggetti a trasferimento verso Paesi terzi (esterni all'Unione europea e all'area economica europea), il trasferimento avviene: • in presenza di una delle condizioni previste dall'art. 43 del Codice? oppure • verso uno dei paesi che assicurano un livello adeguato di protezione (omissis- per un elenco aggiornato dei Paesi si veda qui)? oppure • verso un'impresa statunitense che aderisce al ~~Safe Harbor~~ Privacy Shield (link e riferimento al privacy shield sono inseriti da me e non si trovano sul sito del Garante)? oppure • in presenza di clausole contrattuali standard tra esportatore e importatore (e non solo: aggiornamento qui)? oppure • in presenza di un'autorizzazione ad hoc da parte del Garante?		
7. I doveri del titolare del trattamento in caso di esercizio dei diritti degli interessati ai sensi dell'art. 7 del Codice		
In presenza dell'esercizio del diritto d'accesso, viene dato riscontro all'interessato secondo le modalità previste dalla legge?		

A parere di chi scrive, la checklist sopra riportata è un ottimo strumento per valutare l'impatto della normativa privacy ed individuare le aree in cui si possono rendere necessari degli interventi.

Occorre tener presente che vi sono molte aree che richiedono adempimenti peculiari, come ad esempio l'attività di marketing, la profilazione o la geolocalizzazione, ma è anche vero che, in linea generale, i provvedimenti del Garante danno indicazioni particolari in ordine alla liceità dei trattamenti, alle informazioni da rendere agli interessati, alle modalità con cui rendere l'informativa alla necessità di procedere a notifica o a verifica preliminare, alla necessità di acquisire il consenso al modo in cui deve essere acquisito. Pertanto, anche rispetto a questi trattamenti le aree più critiche sono sempre quelle che risultano dalla lista di controllo, ed è possibile partire da lì per verificare l'eventuale compliance ai provvedimenti ulteriori eventualmente resi dal Garante in materia.

Più la realtà aziendale è complessa, infatti, più la checklist dovrebbe essere estesa. Tuttavia per le piccole realtà, si ribadisce, può costituire un ottimo strumento di partenza.

Sia chiaro che, rispondere sì a tutte le domande non mette al riparo da tutte le possibili violazioni, ma certamente indica che si è sulla buona strana per prevenirle.

D'altro canto, rispondere no alla maggior parte dei quesiti, denota una forte carenza della conoscenza della disciplina, e una conseguente carenza di conformità agli adempimenti di legge: una prima mappatura delle lacune consente anche di dare una lettura più consapevole della normativa, potendo rivolgere lo sguardo anche all'applicazione pratica delle regole canonizzate dal legislatore.

La checklist dell'ICO

Partendo da questo presupposto, cioè che la checklist sia un ottimo sistema per saggiare la conoscenza della normativa applicabile alla propria realtà e dare una lettura "pratica" dei codici e delle norme che possono scaturirne, avrei voluto suggerire la lettura della lista di controllo formulata dall'ICO, che, però, soffre del fatto che, se non si è ben consapevoli delle discrepanze tra le normative nazionali di riferimento, rischia di essere fuorviante. Pertanto ho deciso di riadattarla al nostro quadro, provando a conservarne il linguaggio semplice e l'approccio immediato, creando l'infografica sulla check list privacy qui sotto.

Un altro strumento davvero valido messo a disposizione dall'ICO, che consente anche di saggiare il livello di sicurezza informatica, è il "Data protection self assessment toolkit": occorre però anche qui tener ben presente la differenza tra le normative dei due Stati (resta comunque utilissima la parte sulla sicurezza informatica, al di là delle misure minime).


Checklist Privacy
Ho davvero bisogno di queste informazioni personali? So per cosa intendo usarle? So che esistono differenze nel modo in cui vanno trattati i diversi tipi di dati personali (ad esempio dati personali, dati sensibili o giudiziari)?
Le persone alle quali queste informazioni sono riferite, sanno che le tratto? Hanno capito per cosa saranno usate?
Sono certo che i dati personali siano sicuri e protetti? Sono protetti sia quando li tratto in cartaceo sia quando li tratto attraverso computer o altri device? Mantengo il controllo sui diversi strumenti? Il mio sito è sicuro?
Sono certo che i dati personali che tratto siano accurati e aggiornati?
Cancello le informazioni di cui non ho più bisogno, non appena mi accorgo di non avere più bisogno? Ho stabilito i tempi di conservazione dei dati?
L'accesso ai dati personali è limitato alle sole persone che hanno necessità di averne conoscenza?
http://
Se ho bisogno di diffondere i dati personali di qualcuno sul web, compresi quelli dei miei dipendenti, gli do le necessarie informazioni? Raccolgo i consensi?
Sto disciplinando l'uso di internet e della strumentazione elettronica? Se faccio controlli o monitoro la strumentazione o le comunicazioni elettroniche (ad esempio: monitoro le email dei miei dipendenti), sono certo di poterlo fare? So in che limiti posso monitorare le email? Ho informato i dipendenti di questa attività, gli ho spiegato in quali circostanze avviene o perché? Sono sicuro di non violare lo Statuto dei lavoratori o la segretezza della corrispondenza?
Ho istruito adeguatamente i miei dipendenti o i fornitori esterni sui loro compiti e doveri? So in quali casi si possono impartire istruzioni orali agli incaricati? I fornitori esterni sono stati nominati responsabili oppure sono contitolari o titolari autonomi? Ho dei subcontraenti o sono io stesso un subcontraente (es. subappalto)? Sono stati nominati responsabili (o sono stato nominato responsabile)? So che anche in questi casi solo il titolare può nominare i responsabili?