

2. TEST VALUTAZIONE (PER TUTTA L'ORGANIZZAZIONE)**2.1 QUALITÀ DEI DATI**

Il Testo Unico della Privacy mira a sviluppare una nuova cultura del trattamento dei dati. (è introdotto il principio, in base al quale, i dati devono essere esatti, completi ed aggiornati).

Elemento di valutazione		Risultato / Commento
1.1	Le informazioni detenute sono accurate, nel senso che non contengono errori?	
1.2	Vengono predisposte delle misure di verifica periodica o automatizzata della correttezza dei dati e del loro aggiornamento?	
1.3	Una volta che si riceve comunicazione dell'avvenuta variazione di un dato personale, si è certi che ne venga a conoscenza l'incaricato che lo tratta?	

2.2 MODALITÀ DELLA RACCOLTA

Nel Testo Unico della Privacy viene suggerito in che modo, per i dati raccolti, si debbano rispettare i criteri di liceità, determinatezza, specificità e pertinenza. In questa fase, oltre che ad un confronto con le finalità del trattamento, è necessario che il dato sia raccolto con il massimo della trasparenza e senza artifici messi in atto, a danno dell'interessato.

Elemento di valutazione		Risultato / Commento
2.1	Il dato raccolto è conforme alla legge, ai regolamenti ed alle normative comunitarie che interessano l'organizzazione?	
2.2	I dati raccolti sono conformi con i fini istituzionali dell'organizzazione?	
2.3	Il dato è stato raccolto rispettando la massima trasparenza con l'interessato? L'informativa era chiara? La modalità di utilizzo del dato era sufficientemente manifesta?	

2.3 MISURA DELLA SICUREZZA

Analizzare le misure di sicurezza che vengono applicate all'intero processo di trattamento dei dati, sui tre livelli: organizzativo, fisico e logico. Le misure di sicurezza devono essere adeguate in modo da garantirsi contro i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta. Il giudizio di conformità delle misure, passa attraverso la valutazione dello stato della tecnologia, rapportato alla natura dei dati e alle conseguenze che deriverebbero da eventuali distruzioni illecite dei dati o da eventuali effrazioni.

Elemento di valutazione		Risultato / Commento
3.1	Si sono analizzate le possibilità di accesso fisico ai locali e agli elaboratori in essi contenuti?	
3.2	Si sono analizzate le possibilità di accesso logico agli elaboratori? Di accesso alla rete interna, dall'esterno? Di accesso all'esterno, dalla rete interna?	
3.3	Vengono effettuate procedure di back-up e conservazione delle copie?	
3.4	Agli operatori che lavorano con i computer, viene assegnata una password di accesso?	
3.5	Per ogni password, viene definito un profilo utente che permette di accedere solo ai dati strettamente necessari alle sue mansioni?	
3.6	Esistono controlli antivirus?	
3.7	I dati sensibili vengono archiviati separatamente da quelli manuali?	
3.8	I dati sono contenuti in armadi non accessibili o in locali sorvegliati?	
3.9	Si effettuano delle ispezioni periodiche che permettono di verificare la correttezza del trattamento?	

2.4 FIGURE DI RIFERIMENTO

L'individuazione delle figure di riferimento (Titolare, Responsabile/i, Incaricato/i) legata alla definizione dei ruoli all'interno del processo di trattamento, è l'operazione per stabilire "chi fa che cosa". In tal senso, torna utile la redazione di appositi mansionari, indicanti le procedure di accesso ai dati, le metodologie di trattamento e le misure di sicurezza da rispettare.

Elemento di valutazione		Risultato / Commento
4.1	È stata analizzata l'articolazione interna all'organizzazione, per area funzionale e per divisioni territoriali?	
4.2	Si ritiene opportuno nominare uno o più responsabili, al fine di delegare alcune funzioni, per una maggiore garanzia di un'applicazione corretta della legge?	
4.3	Si è provveduto a redigere il/i mansionario/i da rilasciare al/ai responsabile/i ed eventualmente agli incaricati?	
4.4	Si ritiene opportuna una relazione periodica da parte dei responsabili circa l'andamento dell'applicazione della legge, al fine di avere una maggiore cognizione delle esigenze applicative?	
4.5	Si è provveduto alla formazione dei Responsabili e degli incaricati?	

2.5 INFORMATIVA

L'informativa è il documento principale che legittima la raccolta dei dati ed in generale il loro trattamento. Tale documento, è da rilasciare all'interessato (cliente, dipendente, fornitore, utente, etc) al momento della raccolta dei dati: esso deve indicare con estrema trasparenza e dettaglio, le finalità e le modalità del trattamento ed eventuali ambiti di comunicazione e diffusione dei dati.

Elemento di valutazione		Risultato / Commento
5.1	E' stato predisposto l'Informativa da rilasciare agli interessati e sono state date indicazioni sul suo corretto utilizzo ?	
5.2	Ogni volta che viene raccolto un dato personale viene rilasciata l'informativa, scritta o verbale? La persona incaricata dispone della formazione necessaria per gestire correttamente questa fase?	
5.3	L'interessato a cui è rivolta l'informativa è in grado di capire la terminologia utilizzata e di comprendere chiaramente il destino futuro del suo dato?	
5.4	L'informativa contiene tutti gli elementi indicati dalla normativa (ex comma 1 dell'art. 10) ?	
5.5	Si effettuano dei controlli periodici per verificare la conformità del trattamento del dato personale con l'informativa rilasciata all'interessato di merito?	

2.6 Consenso

Salvo i casi di esclusione del consenso la possibilità di trattamento dei dati, dopo il rilascio dell'informativa, è condizionata al conferimento del consenso dell'interessato documentato per iscritto, o altro requisito equipollente per il trattamento dei "dati comuni"; al consenso scritto dell'interessato, per il trattamento di dati sensibili.

Elemento di valutazione		Risultato / Commento
6.1	Si provvede ad ottenere il consenso prima di cominciare a trattare il dato?	
6.2	Il consenso è sempre preceduto da una chiara informativa?	
6.3	L'interessato è messo nelle condizioni di prestare liberamente il suo consenso?	
6.4	Si pone il blocco ai dati personali per il quale non si è ancora ottenuto il consenso?	

2.7 AUTORIZZAZIONI

Richiesta di Autorizzazione al Garante per il trattamento dei dati sensibili.

Elemento di valutazione		Risultato / Commento
7.1	Tra le sei Autorizzazioni generali sono state analizzate quelle riguardanti i dati sensibili che vengono trattati all'interno dell'organizzazione?	
7.2	È stata posta la dovuta attenzione ai limiti delle Autorizzazioni, cioè ai confini entro il quale rimane possibile trattare un particolare dato sensibile senza dover chiedere un'Autorizzazione specifica al Garante	

2.8 NOTIFICAZIONE

E' una dichiarazione esaustiva di tutte le operazioni che vengono effettuate all'interno della realtà aziendale. Questo documento, permette l'istituzione di un "registro dei trattamenti" presso l'ufficio del Garante (Roma), il cui scopo, è quello di censire tutte le tipologie di trattamenti esistenti sul territorio nazionale.

Elemento di valutazione		Risultato / Commento
7.1	È stato notificato al Garante nei tempi stabiliti dalla legge?	
7.2	Vengono predisposti controlli periodici per verificare l'attualità di ciò che era stato precedentemente dichiarato? Se qualcosa è cambiato, si è provveduto ad una nuova notificazione al Garante?	

EVENTUALI NOTE

--