

Argomento / quesito	F/O	Procedura presente in azienda	
		SI	NO
*** Notifica al Garante			
Si è verificato se la ditta effettua trattamenti tali da richiedere l'effettuazione della notifica al Garante? Analizzare i tipi di trattamento citati nell'articolo 37, che stabiliscono l'eventuale obbligo di notifica.	F		
*** Responsabili trattamento dati			
E' stata valutata l'opportunità di nominare un Responsabile privacy del trattamento dei dati personali?	F		
SE è stato nominato uno o più responsabili, interni e/o esterni, è stata compilata una nomina formale e circostanziata, riportante tutte e solo le incombenze a lui riservate, e la nomina è stata firmata per accettazione ed allegata agli atti?	O		
*** Incaricati trattamento dati			
E' stata elaborata la lista degli incaricati, prendendo in considerazione tutte e solo le persone fisiche che interagiscono con i dati personali? I componenti della lista sono stati formalmente nominati?	O		
Ai collaboratori individuati come incaricati e per i quali è previsto un accesso al sistema informatico, sono state assegnate delle credenziali di autenticazione? (codice per l'identificazione dell'incaricato associato ad una password, oppure dispositivo di autenticazione...caratteristica biometrica...)	O		
Ad ogni incaricato nominato, o per classi omogenee di incaricati, è stato attribuito un profilo di autorizzazione , riportante le banche dati (v "Banche dati") alle quali può accedere, con il dettaglio dell'ambito del trattamento concesso? (obbligatorio quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso, anche se solo per l'accesso ai dati cartacei).	O		
La lista degli incaricati viene almeno annualmente controllata? (revisione / verifica profili, sussistenza condizioni...).	O		
Vengono immediatamente soppresse le credenziali in caso di perdita delle qualità che consentono l'accesso ai dati (dimissioni, cambio mansioni...), oppure in caso di mancato utilizzo per 6 mesi delle credenziali stesse?	O		
Sono stati individuati incaricati ai quali attribuire compiti specifici, come: amministratore di sistema, incaricato salvataggi, custode password?	F		
La password è formata da almeno 8 caratteri, scade almeno ogni 6 mesi (3 in caso di trattamento di dati sensibili), è conosciuta solo dall'incaricato, e non contiene riferimenti agevolmente riconducibili all'incaricato stesso?	O		
Agli incaricati sono state date adeguate istruzioni scritte riportanti le principali regole di correttezza e cautela nel trattamento di dati, in particolare, ma non solo, per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento?	O		
*** Banche dati			

E' stata fatta una lista delle banche dati , elettroniche e cartacee, contenenti dati personali comuni e/o sensibili-giudiziari?	<input type="radio"/>		
Questa lista è chiaramente propedeutica all'assegnazione dei profili ai vari incaricati.			
*** Lista dispositivi elettronici:			
E' stata fatta una lista dei dispositivi elettronici , almeno di quelli che memorizzano i dati e che quindi influenzano la relativa sicurezza, mettendo in evidenza le principali caratteristiche riguardanti la sicurezza, come il sistema operativo, i dispositivi di back up, la presenza di un antivirus adeguato...?	<input type="radio"/>		
*** Formazione			
E' stata fatto un programma di formazione degli incaricati del trattamento, prevedendo sessioni di formazione , svolta da personale qualificato e/o (almeno) è stato consegnato adeguato materiale formativo / informativo a ciascun incaricato?	<input type="radio"/>		
E' assolutamente consigliato riportare traccia delle operazioni di formazione effettuate con la compilazione di "verbali di formazione" e "liste di distribuzione" del materiale didattico, riportante le firme degli incaricati.			
*** Informative			
E' stata predisposta un'adeguata informativa per i clienti/fornitori? E per i dipendenti/collaboratori?	<input type="radio"/>		
Controllare se nell' informativa sono considerati TUTTI i requisiti previsti dall'art. 13. Ricordarsi, nel caso in cui l'informativa non richiede il consenso scritto da parte del soggetto interessato, che occorre documentare l'avvenuta consegna.			
Sono state esaminate tutte le forme di richiesta dati usate in ditta e quindi suscettibili di essere corredate da informativa?	<input type="radio"/>		
Conservazione curriculum, form di richiesta dati sul sito aziendale, moduli di richiesta dati distribuiti in fiere, consegnati ad agenti ecc ecc.			
** Terze parti			
Sono stati individuati, analizzati, e regolati i processi che prevedono la partecipazione di terze parti nella gestione dei dati personali aziendali?	<input type="radio"/>		
Es. consulente paghe, commercialista, società di informatica ecc Da curare in particolare trasferimento di dati in paesi terzi.			
Sono state chieste alle terze parti individuate le opportune garanzie per un trattamento dati conforme alla normativa della privacy?	<input type="radio"/>		
*** Video sorveglianza			
Se presente dispositivo di video sorveglianza, sono stati esposti i cartelli di segnalazione?	<input type="radio"/>		
E' stata studiata la normativa relativa alla video sorveglianza (luoghi controllati, periodo di conservazione riprese...) prendendo anche in considerazione gli ovvi punti di sovrapposizione con lo statuto dei lavoratori (art. 4 comma 1).	<input type="radio"/>		
*** Altre misure minime di sicurezza			
Tutti i PC che trattano in qualche modo dati personali, anche se non in rete, sono dotati di antivirus correttamente e regolarmente aggiornati?	<input type="radio"/>		
Viene eseguito regolarmente, almeno una volta la settimana, il salvataggio dei dati?	<input type="radio"/>		
S'intendono TUTTI i dati personali, comuni e/o sensibili, risidenti nel server e/o nei clients, aggiornati con software gestionale e/o Software di produttività individuale.			

E' assolutamente consigliabile disporre di una documentazione riportante le principali caratteristiche della procedura di salvataggio.			
E' stata predisposta una procedura, con disposizioni scritte, volte a precisare le modalità con le quali si può assicurare la disponibilità di tutti i dati personali, anche in assenza di qualsivoglia incaricato? Chiaramente questo punto è tassativo quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione.	<input type="radio"/>		
Viene eseguito almeno una volta l'anno (semestralmente in caso di dati sensibili) gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti?	<input type="radio"/>		
Quando ci si avvale di soggetti esterni alla propria struttura per provvedere all'attivazione/manutenzione di quanto attiene al buon funzionamento delle misure minime di sicurezza si riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni previste dalla normativa?	<input type="radio"/>		
*** Caso di trattamento di dati sensibili elettronicamente			
Il documento programmatico sulla sicurezza viene redatto e/o rivisto ogni anno entro il 31 marzo? Il documento deve contenere e soddisfare quanto previsto dal punto 19 dell'allegato B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA Si ricorda inoltre che il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.	<input type="radio"/>		
I dati sensibili o giudiziari sono protetti contro l'accesso abusivo dall'esterno, mediante l'utilizzo di idonei strumenti elettronici (es. firewall)?	<input type="radio"/>		
Supporti removibili: sono state impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti removibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti? I dati sensibili o giudiziari contenuti nei supporti removibili, se non più utilizzati, sono distrutti o resi inutilizzabili oppure i dati precedentemente contenuti sono resi intelligibili e tecnicamente in alcun modo non ricostruibili?	<input type="radio"/>		
Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni?	<input type="radio"/>		
*** Trattamenti senza l'ausilio di strumenti elettronici			
Sono state impartite agli incaricati, anche se trattano dati nella sola modalità cartacea, istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali?	<input type="radio"/>		
L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato, e le persone che vi accedono devono essere preventivamente autorizzate. E' stato predisposto un registro dove identificare e registrare persone ammesse agli archivi soprannominati in particolare dopo l'orario di chiusura?	<input type="radio"/>		