Allegato D
Scheda usata per il rilevamento dei trattamenti

© COMUNE DI SALA CONSILINA – 2011

(da compilare in ogni sua parte e restituire al Dirigente Responsabile)

Informativa ai sensi art. 13 Dlgs 196/03 "I dati contenuti nel presente questionario saranno utilizzati unicamente ai fini dell'analisi dei rischi connessi ai trattamenti di dati personali in essere e per l'adozione delle misure di sicurezza necessarie alla protezione dei dati personali da ciascuno trattati. Essi non verranno comunicati ad alcuno, tranne che alla società incaricata di sovrintendere alle risorse del sistema operativo dei nostri elaboratori e di provvedere alla manutenzione software, per l'adozione delle necessarie misure di sicurezza e per la redazione del DPSS."

Settore/area	
Servizio	
Ufficio	
Responsabile	*Nome e cognome del responsabile dell'ufficio*
Dati rilevati da	*Nome e cognome di chi ha rilevato i dati*

Schede dei trattamenti di dati COMUNI di competenza dell'ufficio relativi a DATI PERSONALI

Indicare quali, tra i procedimenti di competenza dell'ufficio, trattino dati personali COMUNI ovvero diversi da quelli SENSIBILI o GIUDIZIARI, compilando una scheda per ogni gruppo di procedimenti omogeneo ovvero che ha le caratteristiche analoghe tra quelle richieste.

(COMPILARE UNA SCHEDA PER OGNI TRATTAMENTO identificando ciascuna con il "Numero progressivo della scheda")

N. scheda	*Numero progressivo della scheda*	**Codice Trattamento**	*Non compilare*
Denominazione del trattamento	*Descrivere il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es., fornitura di beni o servizi, gestione del personale, ecc.)*		
Categorie interessate	*indicare le categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.)*		
Compiti e responsabilità dell'ufficio	*descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.).*		
Riferimenti normativi	*riferimenti normativi, atti o altri documenti già predisposti (provvedimenti, ordini di servizio, regolamenti interni, circolari), indicando le precise modalità per reperirli*		
Elenco altri uffici coinvolti	*altre strutture che concorrono al trattamento, anche dall'esterno..*		
Strumenti utilizzati	*va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi).*		
Banca dati	*indicare eventualmente la banca dati (ovvero il data base o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i dati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso occorre elencarle tutte.*		
Ubicazione supporti	*indicare de i dati sono gestiti LOCALMENTE e quindi su quali PC risiedono e come e dove vengono eseguire le copie di sicurezza. Nel caso i dati siano in sistemi centrali gestiti dal CED, indicare semplicemente "CED"*		
Tipologia di connessione	*Tipologia di interconnessione: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: nessuna, rete locale, geografica, Internet, ecc*		

(COMPILARE UNA RIGA per ogni Minaccia relativa ai trattamenti sopra elencati – Nel caso una minaccia si riferisca solo ad alcuni trattamenti, indicare nelle colonna "Gravità" la frase: "Solo per i trattamenti n. x, y, …")

Elencare eventuali minacce percepite alla sicurezza dei dati seguendo lo schema seguente			
Descrizione minaccia	**Vulnerabilità**	**Gravità**	**Contromisure usate/da usare**
descrizione dell'evento che può generare danni e che comporta, quindi, rischi per la sicurezza dei dati personali	*Indicare le cause che favorirebbero l'attuazione della minaccia*	*Indicare la gravità della minaccia specificando i danni che essa provocherebbe*	*Indicare se sono già in atto delle contromisure per contrastare le minacce ed eventualmente suggerirne altre da attuare*

Scheda di Autoanalisi delle Misure di sicurezza esistenti

(fare una ricognizione della situazione attuale media della postazioni del proprio ufficio, secondo le proprie conoscenze)

- Il proprio computer e le proprie applicazioni sono dotate di **"password"** personale per l'accesso ai dati personali?

☐ **SI** ☐ **NO** ☐ **NO per le seguenti applicazioni ……..**

- Lei è in grado, qualora lo desideri, di **cambiare autonomamente la "password"** di accesso al proprio elaboratore o alle applicazioni che gestiscono i dati personali?

☐ **SI** ☐ **NO** ☐ **NO per le seguenti applicazioni …….....**

Se **SI**, con quale periodicità viene cambiata la password …….....

- Le è stato attribuito un **"codice identificativo personale"** (detto user-id o user-name o nome utente) ☐ **SI** ☐ **NO**

Se Si, quale? **……** (es. PAOLOR, BIANCHIG, ….)

- Gli armadi o classificatori in cui sono conservati i dati personali su supporto cartaceo, sono **dotati di serratura** la cui chiave è in possesso dell'incaricato autorizzato al loro trattamento ed il dirigente responsabile? ☐ **SI** ☐ **NO**
- Se ha un PC, utilizza il lettore di floppy disc o CD-ROM per conservare dati personali ☐ **SI** ☐ **NO**

  In caso affermativo, i supporti informatici sui quali sono contenuti dati personali (dischetti di back-up) sono conservati **in armadio o cassetto con serratura**, la cui chiave è in possesso dell'incaricato autorizzato al loro trattamento e del dirigente? ☐ **SI** ☐ **NO**

- Utilizza le cartelle sul server centrale per conservare i dati personali o salva tali dati sul suo PC? ☐ **SI** ☐**NO**
- Ha un modem sul suo PC necessario per espletare alcune mansioni? ☐ **SI** ☐ **NO**

  Se si, conosce i rischi di sicurezza informatica ad esso associati ☐ **SI** ☐ **NO**
- Ha necessità di utilizzare il collegamento ad Internet per esigenze di lavoro? ☐ **SI** ☐ **NO**

  Se si, conosce i rischi i rischi di sicurezza informatica connessi alla navigazione Internet? ☐ **SI** ☐ **NO**
- Ha necessità di utilizzare la posta elettronica per esigenze di lavoro? ☐ **SI** ☐ **NO**

  Se si, conosce i rischi i rischi di sicurezza informatica connessi all'uso di tale strumento? ☐ **SI** ☐ **NO**

- Quali **altre misure di sicurezza** di carattere organizzativo, fisico o logico esistono nel proprio ambiente o nella propria postazione di lavoro? (descrivetele qui di seguito brevemente: es. impianto antincendio, controllo accessi, …)

……

……

- In base alla propria esperienza ed alle caratteristiche del proprio posto di lavoro, quali altre misure di sicurezza di carattere organizzativo, fisico o logico si **possono suggerire**? (descrivetele qui di seguito brevemente)

……

……

- Altre note personali …….

Esempi di minacce e vulnerabilità comuni

Minacce	Vulnerabilità
sottrazione di credenziali di autenticazione	Assenza di adeguata formazione agli operatori sull'uso dei sistemi comunali
	Conservazione password non adeguata
	Assenza di aggiornamento periodico delle password
	Password troppo semplici
Rivelazione/diffusione di dati sensibili e/o giudiziari	Carenza di consapevolezza, disattenzione o incuria
	Assenza di adeguata formazione agli operatori sull'uso dei sistemi comunali
	Mancanza di atti formali di responsabilizzazione degli incaricati
comportamenti sleali o fraudolenti	Assenza di infrastrutture tecniche di sicurezza (inferriate, sistemi di allarme perimetrale, sorveglianza, etc).
errore materiale	Privilegi di accesso errati ai sistemi informatici comunali
	Assenza di adeguata formazione agli operatori sull'uso dei sistemi comunali
	Assenza di automazione nelle attività di caricamento dati per informazioni già in possesso del Comune
	Errori di scrittura degli operatori comunali
azione di virus informatici o di programmi suscettibili di recare danno	Applicazioni di controllo della sicurezza non correttamente configurate o non adeguate allo stato dell'arte
	Mancanza di antivirus/antispyware aggiornati
spamming o tecniche di sabotaggio	Assenza di filtri antispam aggiornati periodicamente
	Non adeguato controllo degli accessi alle postazioni di lavoro e/o agli uffici
	Applicazioni di controllo della sicurezza non correttamente configurate o non adeguate allo stato dell'arte
malfunzionamento, indisponibilità o degrado degli strumenti	Mancanza di un piano di manutenzione adeguato Mancanza di un piano finanziario per l'adeguamento tecnologico del parco macchine
accessi esterni non autorizzati	Non adeguato controllo degli accessi alle postazioni di lavoro e/o agli uffici
	Mancanza di un sistema di rilevamento delle intrusioni
	Gestione scorretta o mancanza di firewall ed accessi concessi ad esterni senza adeguato controllo o supervisione
	Inadeguatezza delle policy di riservatezza nei contratti di servizi con fornitori esterni
intercettazione di informazioni in rete	Mancanza di sistemi che rilevino, in tempo reale, eventi su rete non autorizzati
	Mancanza di sistemi di crittografia per la trasmissione e conservazione di dati sensibili e/o giudiziari
ingressi non autorizzati a locali/aree ad accesso ristretto	Non adeguato controllo degli accessi alle postazioni di lavoro e/o agli uffici
	Mancanza di sistemi serrature, lucchetti o altri sistemi di protezione analoghi
sottrazione di strumenti contenenti dati	Non è prevista esplicita autorizzazione per il prelievo degli apparati
	Non adeguato controllo degli accessi alle postazioni di lavoro e/o agli uffici
	Mancanza di casseforti o altri depositi di sicurezza
eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...)	Presenza di materiali infiammabili quali carta o scatoloni Assenza di verifiche statiche sulle strutture e/o del rischio sismico Inadeguatezza degli impianti di mesa a terra, salvavita o antifulminazione
	Vicinanza a corsi d'acqua o bacini
	Conservazione risorse in cantine o sotterranei soggetti ad allagamento
	Non adeguata politica di conservazione dei supporti per le copie di sicurezza
	Collocazione delle apparecchiature a livello del pavimento
eventi distruttivi dolosi, accidentali o dovuti ad incuria	Presenza di materiali infiammabili quali carta o scatoloni Sistema antincendio inadeguato alle tipologie di risorse da salvaguardare
guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Assenza di verifiche periodiche sull'impianto elettrico Non adeguata manutenzione degli impianti
errori umani nella gestione della sicurezza fisica	Mancanza di strumenti di verifica controllo
	Assenza di adeguata formazione agli operatori addetti alla sicurezza