

GUIDA OPERATIVA PER LA REDAZIONE DEL DPS

REGOLA 19D.LG. 30/6/2003 N. 196

Tabella 1.1 - Elenco dei trattamenti: informazioni essenziali

ESEMPI

Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	Sensibili	Giudiziari			
Fornitura di servizi tecnici	Clienti	No	No	Studio tecnico	Tecnico informatico	Computer, rete locale, collegamento ad Internet
Consulenze tecniche	Clienti	No	No	Studio tecnico	Tecnico informatico	Computer, rete locale, collegamento ad Internet
Gestione personale	Dipendenti e/o collaboratori	No	No	Studio tecnico	Consulente del lavoro, Tecnico informatico	Computer, rete locale, collegamento ad Internet
Gestione acquisti	Fornitori	No	No	Studio tecnico	Commercialista, Tecnico informatico	Computer, rete locale, collegamento ad Internet

Tabella 1.2 - Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti

ESEMPI

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
01 – Fornitura di servizi tecnici	Softwares applicativi (es. anche documenti Word)	Studio tecnico (sale di lavoro, archivi, ecc.)	PC fisso e/o portatile	Rete locale, Internet
02 – Consulenze tecniche	Softwares applicativi (es. per consulenze sulla sicurezza del lavoro)	Studio tecnico (sale di lavoro, archivi, ecc.)	PC fisso e/o portatile	Rete locale, Internet
03 – Gestione personale	Softwares gestionali (personale)	Studio tecnico (sale di lavoro, archivi, ecc.)	PC fisso e/o portatile	Rete locale, Internet
04 – Gestione acquisti	Softwares gestionali (acquisti)	Studio tecnico (sale di lavoro, archivi, ecc.)	PC fisso e/o portatile	Rete locale, Internet

Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti

ESEMPI

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Studio tecnico	01 – 02 – 03 – 04	Acquisizione e caricamento dei dati, comunicazione a terzi, gestione tecnica operativa delle base dati (salvataggi ripristini ecc.), eventuale manutenzione tecnica dei programmi.
Consulente del lavoro	03	Acquisizione e caricamento dei dati, gestione tecnica operativa delle base dati (salvataggi ripristini ecc.), eventuale manutenzione tecnica dei programmi.
Commercialista	04	Acquisizione e caricamento dei dati, gestione tecnica operativa delle base dati (salvataggi ripristini ecc.), eventuale manutenzione tecnica dei programmi.
Tecnico informatico	01 – 02 – 03 – 04	manutenzione tecnica dei programmi e apparecchiature elettroniche

Tabella 3 – Analisi dei rischi

(ESEMPIO DI ANALISI)

	Rischi	Si No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa) (gravità = probabilità x rilevanza)
Comportamenti degli operatori	Sottrazione di credenziali di autenticazione	Si	Possibile accesso ai dati da parte di persone non autorizzate. Media
	Carenza di consapevolezza, disattenzione o incuria	Si	Possibile fuoriuscita di dati, per esempio contenuti su eventuali copie di documenti non utilizzati o su supporti rimovibili che vengono lasciati incustoditi, ovvero perché si lascia incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dati. Alta
	Comportamenti sleali o fraudolenti	Si	Possibile Fuoriuscita o perdita di dati, a causa per esempio di comportamenti scorretti da parte di persone autorizzate, ovvero da parte di persone addette alla manutenzione. Bassa
	Errore materiale	Si	Possibili fuoriuscite di dati, causati per esempio da errori nelle operazioni di copia/taglia/incolla su files o dall'utilizzo di files origine per produrre nuovi files, ecc. Alta
	Altro evento		
Eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno	Si	Possibile perdita di dati. Alta
	Spamming o tecniche di sabotaggio	Si	Possibili perdite o fuoriuscite di dati, causate per esempio da programmi di posta elettronica. Alta
	Mal funzionamento, indisponibilità o degrado degli strumenti	Si	Possibile perdita di dati, causata per esempio da strumenti elettronici obsoleti o di scarsa qualità. Alta
	Accessi esterni non autorizzati	Si	Possibili perdite o fuoriuscite di dati, causate per esempio dall'utilizzo di strumenti elettronici collegati ad Internet che possono essere soggetti ad accessi non autorizzati (hackers). Media
	Intercettazione di informazioni in rete	Si	Possibile fuoriuscita di dati, causata per esempio da cattiva gestione di passwords utilizzate per usufruire di servizi presenti in rete. Alta
	Altro evento		
Eventi relativi al contesto fisico-ambientale	Accessi non autorizzato a locali/reparti ad accesso ristretto	Si	Possibile accesso ai dati o sottrazione degli stessi da parte di persone non autorizzate. Bassa
	Sottrazione di strumenti contenenti dati	Si	Possibile perdita e sottrazione di dati, causata per esempio da furti o da accidentale o dolosa sottrazione di supporti rimovibili quali CD o floppy disk. Media
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	Si	Possibile perdita di dati causata da eventi molto improbabili ma di estrema rilevanza. (Eventualmente si può fare riferimento ad un documento di gestione delle emergenze previsto dal D. Lgs. 626/94). Media
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Si	Possibile perdita di dati, causata per esempio da una scarsa manutenzione degli impianti o da black out. Media
	Errori umani nella gestione della sicurezza fisica	Si	Possibile perdita di dati, a causa per esempio di un cattivo posizionamento di strumenti elettronici o supporti rimovibili (esempio vicino a magneti, telefoni cellulari). Bassa
	Altro evento		

Tabella 4.1 – Le misure di sicurezza adottate o da adottare**ESEMPI**

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare (*)	Struttura o persone addette all'adozione
Utilizzo di programmi antivirus sempre aggiornati	Azione di virus informatici	01 – 02 – 03 – 04	Si		Persone autorizzate al trattamento dei dati
Utilizzo di programmi (tipo Firewall) contrastanti accessi esterni	Accessi esterni non autorizzati, spamming o tecniche di sabotaggio	01 – 02 – 03 – 04	Si		Persone autorizzate al trattamento dei dati
Utilizzo di password o codici identificativi per l'accesso agli strumenti elettronici in genere o a software particolari	Accessi non autorizzati	01 – 02 – 03 – 04	Si		Persone autorizzate al trattamento dei dati
Periodico cambiamento delle password o dei codici identificativi	Sottrazione di credenziali di autorizzazione, intercettazione di informazioni in rete	01 – 02 – 03 – 04	Si		Persone autorizzate al trattamento dei dati
Stanze d'archivio (anche di copie di backup) ad accesso limitato	Accessi non autorizzati, Sottrazione di strumenti contenenti dati	01 – 02 – 03 – 04	Si		Persone autorizzate al trattamento dei dati

(*) Indicare eventualmente i tempi previsti per l'adozione delle misure

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n.		Compilata da		Data di compilazione	
Misura					
Descrizione sintetica					
Elementi descrittivi					
Data aggiornamento					

Da compilare facoltativamente

Tabella 5.1 – Criteri e procedure per il ripristino della disponibilità dei dati

ESEMPIO

Ripristino		
Banca / data base / archivio di dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
Banca dati di software si consulenza sulla sicurezza	Salvare settimanalmente la banca dati in supporto rimovibile, conservare i supporti in archivio ad accesso limitato, ripristinare la banca dati qualora vada danneggiata o persa.	Verificare mensilmente il buon funzionamento di supporti rimovibili necessari al ripristino della banca dati

Tabella 5.2 – Criteri e procedure per il salvataggio dei dati

ESEMPIO

Salvataggio			
Banca dati	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio
Banca dati di software si consulenza sulla sicurezza	Salvare settimanalmente la banca dati in supporto rimovibile	Archivio ad accesso limitato	Titolare del trattamento dei dati, persone autorizzate al trattamento

Da compilare facoltativamente

Tabella 6 – Pianificazione degli interventi formativi previsti

ESEMPIO

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Formazione nuovi addetti al trattamenti dei dati	Nuovi addetti al trattamento dati	1 settimana dall'entrata del nuovo addetto
Formazione per cambiamento di mansione di un addetto	Addetti al trattamento dei dati	1 settimana dal cambiamento di mansione
Formazione per introduzione di nuovi strumenti elettronici o programmi informatici	Addetti al trattamento dei dati	1 settimana dall'introduzione degli strumenti elettronici o dei programmi informatici

Tabella 7 – Trattamenti affidati all'esterno

ESEMPI

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Gestione personale	Trattamento dati del personale	Consulente del lavoro	Rilascio di una dichiarazione che attesti: che il trattamento dei dati ai soli fini dell'espletamento dell'incarico ricevuto; l'adempimento degli obblighi previsti dal Codice per la protezione dei dati personali; il rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere; l'impegno a relazionare periodicamente sulle misure di sicurezza adottate e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.
Gestione acquisti	Trattamento dati di acquisiti da fornitori	Commercialista	IDEM
Manutenzione programmi contenenti dati personali	Tutti i trattamenti dei dati	Tecnico informatico	IDEM

Tabella 8 – Cifratura dei dati o separazione dei dati identificativi (solo per organismi sanitari ed esercenti professioni sanitarie)

Trattamenti di dati	Protezione scelta (Cifratura/Separazione)	Tecnica adottata	
		Descrizione	Informazioni utili

**INFORMATIVA SUL TRATTAMENTO DI DATI PERSONALI
AI SENSI DELL'ART. 13 DEL DECRETO LEGISLATIVO N.196 DEL 30/06/2003
"CODICE IN MATERIADI PROTEZIONE DEI DATI PERSONALI"**

Il sottoscritto Dott. Ing. _____
nato il _____ a _____
codice fiscale _____ partita IVA _____
iscritto all'Ordine degli Ingegneri della Provincia di Trapani, al numero _____
titolare dello Studio _____
sito in _____ via _____
è il titolare nonché il responsabile del trattamento di cui alla presente informativa.
Il sottoscritto con la presente

INFORMA

- che i dati personali dell'interessato (**introdurre tutti i dati del cliente**) di cui verrà in possesso avranno un trattamento sia manuale che informatico esclusivamente finalizzato al compimento del proprio incarico, ovvero la fornitura di servizi o consulenze tecniche;
- che i dati personali richiesti all'interessato ed utilizzati saranno quelli strettamente necessari allo svolgimento del proprio incarico;
- che il conferimento dei dati per le finalità sopra indicate è necessario per la corretta esecuzione del proprio incarico, e che qualora l'interessato rifiutasse di fornire i dati richiesti il sottoscritto professionista sarebbe impossibilitato a proseguire nel proprio incarico;
- che tali operazioni di trattamento dei dati personali avvengono rispettando scrupolosamente i principi di riservatezza e di sicurezza richiesti dalla Legge sopra richiamata ed ispirandosi ai principi di correttezza e liceità di trattamento che il sottoscritto ha fatto propri;
- che i suddetti dati personali potranno essere comunicati agli Enti od Organismi competenti, il cui parere, autorizzazione, concessione ecc. sono necessari al corretto e positivo svolgimento dell'incarico professionale; i dati possono inoltre venire a conoscenza di dipendenti o collaboratori dello studio professionale espressamente autorizzati ed incaricati del trattamento dei dati;
- che rispetto ai dati in possesso del sottoscritto, l'interessato potrà sempre esercitare i diritti previsti dall'art.7 della citata Legge, qui di seguito riportato.

_____, li _____

Firma

ART.7 DEL D.LGS. 30/06/2003 N.196

(DIRITTO DI ACCESSO AI DATI PERSONALI ED ALTRI DIRITTI)

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
 - a) dell'origine dei dati personali;
 - b). delle finalità e modalità del trattamento;
 - c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
 - d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
 - e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
 - a) l'aggiornamento la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
 - b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
 - c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
 - a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
 - b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.)

Il sottoscritto _____ interessato al trattamento dei dati personali di cui alla presente informativa, presta il proprio consenso a detto trattamento.

_____, li _____

Firma