Studio Associato Graffigna & Ravaioli

Documento programmatico sulla sicurezza

Art. 34 ed Allegato B, regola 19, D. Lgs. 30 giugno 2003, n. 196

Dott.ssa Laura Graffigna – Dott. Giorgio Ravaioli
(31 marzo 2009)

Indice

Premessa

Il presente Documento Programmatico sulla Sicurezza (DPS) è redatto ai sensi dell'art. 34, comma 1, lettera g) del D. Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), nei modi previsti dal disciplinare tecnico in materia di misure minime di sicurezza, contenuto nell'allegato B), regola 19, del codice stesso.

Esso si articola su 8 sezioni, contenenti informazioni riguardo a:

1. l'elenco dei trattamenti di dati personali (regola 19.1);
2. la distribuzione dei compiti e delle responsabilità (regola 19.2);
3. l'analisi dei rischi che incombono sui dati (regola 19.3);
4. le misure in essere e da adottare (regola 19.4);
5. i criteri e le modalità per il ripristino della disponibilità dei dati (regola 19.5);
6. la pianificazione degli interventi formativi degli incaricati del trattamento (regola 19.6);
7. i trattamenti di dati personali affidati all'esterno (regola 19.7);
8. la cifratura o la separazione dei dati identificativi (regola 19.8).

1. Elenco dei trattamenti di dati personali

Lo Studio Associato Graffigna & Ravaioli detiene e tratta dati personali (comuni e/o sensibili e/o giudiziari) tutelati dal D. Lgs. 30 giugno 2003, n. 196, esclusivamente per il perseguimento delle seguenti finalità:

1. adempimenti di obblighi di legge, regolamento, normativa comunitaria;
2. adempimenti specifici di obblighi stabiliti da norme civilistiche, previdenziali, fiscali, contrattuali, giuslavoristiche;
3. gestione amministrativa e contabile degli adempimenti;
4. rapporti con Istituti, Enti, professionisti od altri soggetti unicamente per consentire l'espletamento dei compiti assegnati allo Studio;
5. ottemperanza ad obblighi professionali;
6. formazione professionale continua.

Qui di seguito si indicano gli ambiti di trattamento individuati, la tipologia di dati trattati, i soggetti responsabili e incaricati, etc.

Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Altre strutture che concorrono al trattamento (anche esterne)	Descrizione degli strumenti elettronici utilizzati	Codice trattamento
Finalità perseguita / Attività svolta	Categorie di interessati	S	G				
Elaborazione paghe e contributi	Clienti e loro dipendenti e collaboratori	Sì	Sì	Amministrazione e contabilità del personale	___	Elaboratore elettronico e pc collegati in rete locale	A1
Consulenza del lavoro e previdenziale	Clienti e loro dipendenti e collaboratori	Sì	Sì	Servizio consulenza	___	Elaboratore elettronico e pc collegati in rete locale, telefono, telefonino	S1

Tabella 1 Elenco dei trattamenti: informazioni essenziali

Codice trattamento	*Banca dati*	*Ubicazione fisica dei supporti di memorizzazione*	*Tipologia di dispositivi di accesso*	*Tipologia di interconnessione*
A1	*Banca dati programma elaborazione paghe*	*Server rete locale presso sede Studio (v. XX settembre, 3/13, Genova). Copie di sicurezza presso sede Studio e domicilio titolari.*	*Terminali, pc*	*Rete locale*
S1	*Banca dati consulenza*	*Server rete locale presso sede Studio (v. XX settembre, 3/13, Genova). Copie di sicurezza presso sede Studio e domicilio titolari.*	*Pc, portatile*	*Rete locale*

Tabella 2 Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti

2. Distribuzione dei compiti e delle responsabilità

Lo Studio Associato Graffigna & Ravaioli è organizzato funzionalmente secondo l'organigramma riportato in appresso; le informazioni essenziali relative alle strutture coinvolte nei trattamenti di dati personali indicati nel precedente paragrafo, sono riportati sinteticamente nella seguente tabella.

Struttura di riferimento	*Trattamenti effettuati dalla struttura*	*Descrizione dettagliata dei compiti e delle responsabilità della struttura*
Amministrazione e contabilità del personale	*Elaborazione paghe e contributi con cadenza mensile, comunicazioni di legge ad enti ed istituti, adempimenti connessi*	*Acquisizione e caricamento dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica ed operativa della base dati*
Servizio consulenza	*Elaborazione pareri scritti od orali, previa eventuale disamina di documenti; comunicazioni di legge ad enti ed istituti, adempimenti connessi*	*Acquisizione dati, consultazione, comunicazione a terzi, gestione tecnica ed operativa della base dati*

Tabella 3 Distribuzione dei compiti e delle responsabilità: informazioni essenziali

3. Analisi dei rischi che incombono sui dati

L'analisi dei possibili rischi che incombono sui dati personali e/o sensibili e/o giudiziari, trattati dallo Studio Associato Graffigna & Ravaioli con strumenti elettronici, è stata effettuata tenendo conto di diversi fattori, di seguito elencati:

1. analisi della tipologia di dati trattati, circa la loro natura e il loro grado di riservatezza;
2. analisi degli strumenti elettronici adottati per il trattamento dei dati personali e sensibili;
3. analisi delle minacce che incombono sui dati trattati, a causa della loro natura o delle vulnerabilità degli strumenti utilizzati per il trattamento;
4. analisi degli eventuali impatti dannosi per gli interessati, derivanti da un incauto trattamento dei dati personali a questi afferenti.

Il risultato di questa analisi è riportato nella seguente tabella.

Tipi di Rischio	*Rischio da considerare (Si/No)*	*Valutazione del rischio (Livello: Alto/Medio/Basso)*
Sottrazione di credenziali di autenticazione	*Si*	*Basso*
Azione di virus informatici o di programmi suscettibili di recare danno	*Si*	*Medio*
Ingressi non autorizzati a locali/aree ad accesso ristretto	*Si*	*Basso*
Perdita dati a seguito danneggiamento/guasto supporti hardware	*Si*	*Medio*

Tabella 4 Analisi dei rischi che incombono sui dati

A seguito dell'analisi dei rischi che incombono sui dati personali oggetti di trattamento, è stata presa in considerazione la gravità dell'impatto sulla riservatezza, integrità e disponibilità dei dati dei vari eventi dannosi esaminati. In base alla valutazione data, sono state stabilite le idonee misure preventive da porre in essere per contrastare anzitutto i rischi maggiori per la sicurezza dei dati trattati.

4. Misure di sicurezza poste in essere e da adottare

Preso atto dell'analisi e la valutazione del rischio, il presente paragrafo prevede la gestione dello stesso, ovvero la disposizione delle misure e degli interventi da porre in essere al fine di prevenire, contrastare o quanto meno ridurre il rischio che si verifichino gli eventi dannosi precedentemente analizzati.

In questa sezione sono riportate le azioni già adottate in quest'ottica di difesa contro i potenziali attacchi alla sicurezza, ma soprattutto gli interventi da eseguire per i medesimi fini, i quali costituiranno il cuore della programmazione sulla sicurezza.

Di particolare rilievo in quest'ambito sono anche i controlli e le verifiche periodiche, necessari per monitorare la costante efficacia nel tempo delle soluzioni adottate.

Priorità di intervento	*Misure*	*Descrizione dei rischi contrastati*	*Trattamenti interessati*	*Misura già in essere*	*Misura da adottare*	*Struttura o persone addette all'adozione*
1	*Variazione periodica delle password di accesso*	*Sottrazione di credenziali di autenticazione*	*Archivi dati*	*Sì*	*No*	*A1-S1*
2	*Uso combinato del supporto e di password*	*Utilizzo indebito smart card*	*Dati utilizzati negli accessi*	*No*	*Sì*	*A1-S1*
3	*Utilizzo di programmi di protezione (antivirus, firewall, ecc.) costantemente aggiornati*	*Azione di virus informatici o di programmi suscettibili di recare danno*	*Archivi dati*	*Sì*	*No*	*A1-S1*
4	*Chiusura dei locali in assenza di operatori*	*Ingressi non autorizzati a locali/aree ad accesso ristretto*	*Archivi dati, documenti cartacei*	*Sì*	*No*	*A1-S1*
5	*Utilizzo di unità di backup, gruppi di continuità plurimi*	*Perdita dati a seguito danneggiamento/guasto supporti hardware*	*Archivi dati*	*Sì*	*No*	*A1-S1*

Tabella 5 Misure di sicurezza poste in essere e da adottare

Di seguito si riassumono le raccomandazioni rivolte a tutti gli incaricati dei trattamenti effettuati dallo Studio Associato Graffigna & Ravaioli al fine di garantire quanto previsto dal D. Lgs. 30 giugno 2003, n. 196, a protezione dei dati personali.

Il presente Documento Programmatico sulla Sicurezza deve essere portato a conoscenza di tutti gli utenti del sistema. Inoltre, tale documento dovrà essere mantenuto aggiornato a fronte di modifiche apportate al trattamento dei dati effettuati dallo Studio Associato Graffigna & Ravaioli, nonché a seguito di cambiamenti degli strumenti informatici utilizzati al fine del trattamento di tali dati.

5. Criteri e modalità di ripristino della disponibilità dei dati

In questa sezione sono descritti i criteri e le procedure adottate per il salvataggio e il ripristino dei dati in caso di danneggiamento (volontario o involontario), inaffidabilità o indisponibilità della base di dati in cui essi sono organizzati. L'obiettivo è dunque quello di prevenire eventuali danni agli archivi informatici dove i dati sono custoditi e di organizzare le procedure atte al ripristino, nel minor tempo possibile, dei sistemi di trattamento degli stessi. Ciò in conformità alla regola 19.5 dell'allegato B del D. Lgs. 30 giugno 2003, n. 196, la quale prevede "la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento", nonché "l'adozione di 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".

Di seguito sono sintetizzati i criteri e le procedure per il ripristino dei dati, nonché la pianificazione delle prove di ripristino.

Ripristino della disponibilità dei dati		
Banca dati	*Criteri e procedure per il ripristino dei dati*	*Pianificazione delle prove di ripristino*
Banca dati programma elaborazione paghe	*Backup dati giornaliero su disco fisso server e su unità di memoria esterna, copie custodite c/o sede Studio e domicilio titolari; struttura incaricata: A1*	*Mensile*
Banca dati consulenza	*Backup dati giornaliero su disco fisso server e su unità di memoria esterna, copie custodite c/o sede Studio e domicilio titolari; struttura incaricata: S1*	*Mensile*

Tabella 6 Criteri e modalità di ripristino della disponibilità dei dati

6. Pianificazione degli interventi formativi previsti

Il titolare dei trattamenti, Studio Associato Graffigna & Ravaioli, relativamente alla pianificazione degli interventi formativi, ha previsto quanto segue.

Descrizione sintetica degli interventi formativi	*Classi di incarico o tipologie di incaricati interessati*	*Tempi previsti*
Aggiornamento su normativa in materia di tutela della privacy	*Generalità*	*Semestre*
Aggiornamento sulle modifiche alle procedure informatiche di trattazione dei dati	*Generalità*	*Trimestre*

Tabella 7 Pianificazione degli interventi formativi previsti

Gli interventi formativi rivolti agli incaricati dei trattamenti hanno la finalità di rendere loro edotti circa:

1. l'individuazione dell'insorgenza/modifica dei rischi incombenti sulla riservatezza del trattamento dei dati,

2. l'individuazione delle misure e degli interventi da porre in essere al fine di prevenire, contrastare o quanto meno ridurre i predetti rischi.

7. Trattamenti affidati all'esterno

Il titolare dei trattamenti Studio Associato Graffigna & Ravaioli, non ha attualmente affidato la gestione di alcun trattamento di dati a soggetti esterni.

8. Cifratura dei dati o separazione dei dati identificativi

Il titolare dei trattamenti Studio Associato Graffigna & Ravaioli, relativamente ad alcuni trattamenti di dati, ha adottato le seguenti tecniche di cifratura o di separazione dei dati identificativi:

Trattamenti di dati	*Protezione adottata (Cifratura o Separazione)*	*Tecnica impiegata*	
		Descrizione	*Informazioni utili*
Sensibili	*Separazione*	*Conservazione dei documenti e dei dati in archivi separati e diversificazione del supporto utilizzato per l'archiviazione*	*Strutture interessate: A1 – S1*
Giudiziari	*Separazione*	*Conservazione dei documenti e dei dati in archivi separati e diversificazione del supporto utilizzato per l'archiviazione*	*Strutture interessate: A1 – S1*

Tabella 8 Cifratura dei dati o separazione dei dati identificativi: informazioni essenziali

9. Trattamento dei dati senza l'ausilio di strumenti elettronici

Di seguito si riportano le misure minime di sicurezza da adottare a cura del Responsabile e degli incaricati, in caso di trattamento di dati personali senza l'ausilio di strumenti elettronici:

1. conservazione dei dati, dei documenti e degli atti in locali ad accesso limitato e controllato;
2. chiusura dei locali adibiti a conservazione, in assenza di operatori.

Modalità tecniche da adottare, a cura del titolare e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

1. agli incaricati sono impartite istruzioni scritte o verbali 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;

2. quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;

3. l'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, sono preventivamente identificate ed autorizzate.