Il Documento Programmatico sulla Sicurezza in base Normativa sulla "privacy" applicabile agli studi professionali (D. Lgs 196/03)

A cura di Gianfranco Gargani

A seguito delle diverse richieste degli iscritti all'OGT, si è ritenuto opportuno fornire ulteriori indicazioni che guidino il libero professionista ad una corretta stesura del Documento Programmatico sulla Sicurezza. E' opportuno sottolineare che tutti coloro che trattano dati personali (professionisti, aziende, cooperative, associazioni, P.A., scuole, comuni, ospedali, enti pubblici ecc.) devono adeguarsi alla nuova normativa entro il 31/03/06, salvo le vecchie misure di sicurezza che devono essere già in essere. Gli adempimenti risultano diversi a seconda delle dimensioni della struttura e della tipologia di trattamento dati. Occorre ricordare che nello svolgimento della propria attività, il geologo tratta i dati personali degli eventuali dipendenti, dei propri clienti o di terzi per assolvere le finalità collegate alla corretta esecuzione dell'incarico professionale ricevuto ovvero agli altri obblighi imposti dalla legge professionale o dalle normative vigenti. Frequentemente questi dati personali sono comunicati ad altri professionisti, enti, Pubblica Amministrazione per assolvere agli adempimenti di legge; le informazioni trattate, di solito, non sono oggetto di diffusione ai fini dell'assolvimento dei compiti affidati dalla legge o dai clienti al geologo nell'ambito dell'attività allo stesso riservata.

Di seguito verranno elencati gli elementi fondamentali del documento stesso.

Il Documento Programmatico sulla Sicurezza prevede lo sviluppo dei seguenti punti:

- **Introduzione**: essa contiene i dati identificativi dello studio/società, le definizioni utilizzate (es.: sistema informativo, trattamento, dati personali, etc ai sensi del D.Lgs 196/2003), il Titolare dei dati[1], il Responsabile[2] designato ai sensi dell'art. 4 lett. g) del codice, gli eventuali Incaricati al trattamento dei dati;
- **Elenco di trattamenti di dati dello studio/società**: ovvero fornire l'elenco dei trattamenti[3] di dati personali effettuati dalla struttura (19.1 all. B codice);
- **Ruoli, compiti e responsabilità**: risulta opportuno distribuire i compiti e le responsabilità[4] nell'ambito delle strutture preposte al trattamento dei dati. Elencare le informazioni

---

[1] Il titolare svolge le funzioni di "**titolare del trattamento dei dati personali**" e decide riguardo alle modalità di trattamento e agli strumenti utilizzati, ivi **compreso il profilo della sicurezza**. Il titolare può essere una **persona fisica** (ad esempio: professionista singolo), una **persona giuridica** (ad esempio: società tra professionisti) […], **associazione** (ad esempio: associazione tra professionisti) od organismo (art. 4 lett. f) del codice). E' previsto, inoltre, che le decisioni possano essere prese **anche unitamente ad altro titolare** (art. 4 lett. f) del codice).
Il Titolare del trattamento dei dati:

- adotta (art. 31 "codice"), riguardo al trattamento di dati personali, le misure minime di sicurezza (art. 33 "codice") con le modalità previste dal Titolo V, Capo II del "codice" e dal disciplinare tecnico contenuto nell'allegato B) del "codice" stesso;
- adotta il documento programmatico della sicurezza entro il 31 marzo di ogni anno, ai sensi della regola 19 all. B del codice, vigilando sulla sua effettiva applicazione.

In casi particolari il Titolare:

- adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, ricevendo dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico allegato al "codice" (art. 25 all. B "codice");
- verifica l'adeguamento delle misure minime di sicurezza previste per la protezione dei dati personali all'aggiornamento periodico predisposto dal Ministro della Giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore (art. 36 del "codice").

[2] Si tratta della persona (fisica o giuridica) preposta dal Titolare al trattamento dei dati personali.

[3] Per ogni trattamento elencare e descrivere i dispositivi di accesso e le caratteristiche d'interconnessione.

[4] L'accesso ai dati personali e al loro trattamento con strumenti informatici da parte dei soggetti facenti parte delle varie sezioni dello Studio, è regolato in base alle seguenti misure minime di sicurezza:

- **Sistema di autorizzazione** (devono essere specificati l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del **Profilo di autorizzazione** del richiedente (c.d. "sistema di autorizzazione" ex art. 4 g) del codice e artt. 12-14 allegato B del codice);
- **Credenziali di autenticazione**. Si tratta di strumenti che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti (art. 1 all. B "codice"). Le credenziali di autenticazione consistono in un codice per l'identificazione

anagrafiche ed organizzative relative al personale, specificando a quali aree, riguardo il trattamento di dati personali, può accedere, e quali apparecchiature può utilizzare[5] (19.2 all. B codice);

- **Analisi dei rischi che incombono sui dati**: contiene l'analisi dei i rischi[6] che incombono sui dati (19.3 all. B codice)
- **Misure adottate per garantire integrità e disponibilità dei dati**[7]: vengono descritti i criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare (19.7 all. B codice); viene riportato un piano per la protezione fisica delle aree e dei locali, rilevanti ai fini della custodia e accessibilità dei dati (19.4 all. B codice);
- **Ripristino disponibilità dei dati distrutti o danneggiati**: contiene la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni[8] (19.5 e 23 all. B codice);
- **Descrizione delle attività di formazione**: occorre prevedere interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione

---

dell'incaricato ("user ID") che non può essere assegnato ad altri incaricati, neppure in tempi diversi (art. 6 all. B "codice"), associato a una parola chiave riservata conosciuta solamente dal medesimo incaricato (art. 2 all. B "codice");

[5] Ad esempio: Rete informatica con sistema operativo multiutenza (Win2000/NT, MacOS X, Linux). Oppure accesso consentito tramite lettore smart card / firma digitale o ancora chiavi biometriche. In ogni caso, qualsiasi soluzione in grado di permettere accessi differenziati ai dati. Per il trattamento senza l'ausilio di strumenti elettronici: regole 28, 29 e 30 dell'allegato B al codice.

Le password non vanno riportate nel D.P.S. o in qualsiasi altro documento. Esse sono segrete ed i soggetti incaricati della loro custodia vengono preventivamente incaricati per iscritto a svolgere tale compito (art. 10 allegato B codice).

Le credenziali di autenticazione non utilizzate da almeno **sei** mesi (**tre** mesi per dati sensibili e giudiziari) sono **disattivate**, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (art. 7 all. B "codice").

Le credenziali sono **disattivate** anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali (art. 8 all. B "codice").

Ad ogni incaricato possono essere assegnate o associate individualmente **una o più credenziali** per l'autenticazione (art. 3 all. B "codice").

[6] Ad esempio:

- Rivelazione (comunicazione o diffusione) illegittima di informazioni da parte di soggetti interni o terzi;
- Distruzione o perdita dei dati stessi (anche accidentale);
- Accesso non autorizzato ai dati, da parte di soggetti interni non autorizzati ad un determinato trattamento o da parte di terzi;
- Trattamento non consentito di dati da parte di soggetti non abilitati;
- Trattamento eccedente le finalità per le quali i dati sono stati raccolti.

Per ogni punto è necessario mettere in relazione le misure di sicurezza con gli eventi potenzialmente dannosi per la sicurezza dei dati, le possibili conseguenze e la loro gravità. Il riferimento è la regola 19.3 allegato B al Codice.

[7] Queste misure riguardano tutti i tipi di trattamento dati descritti nelle sezioni precedenti; esse comprendono:

- Protezione fisica delle aree e dei locali ai sensi della regola 19.4 allegato B del codice;
- Sicurezza archivio cartaceo;
- Sicurezza per le eventuali aree facilmente accessibili;
- Eventuali impianti di controllo accessi;
- Protezione informatica degli strumenti elettronici ai sensi della regola 19.4 allegato B del codice
- Sistema operativo in uso
- Installazione software in grado di prevenire vulnerabilità e/o correggere difetti degli strumenti elettronici: es patch del sistema operativo (almeno ogni 6 mesi, 3 mesi se il trattamento riguarda dati sensibili o giudiziari);
- Software antivirus installato e regolarmente aggiornato;
- Software firewall installato e regolarmente aggiornato. Un firewall, letteralmente "muro di fuoco" è un software che permette di monitorare ed inibire gli accessi da remoto alla propria rete informatica. E' una misura minima di sicurezza prevista per il trattamento di dati sensibili e/o giudiziari (art. 20 allegato B al codice);

Per ogni punto è necessario compilare una scheda come quelle sopra descritte, con la quale indicare se la misura è già operativa, o da che data è operativa, e verificarne periodicamente l'efficienza.

[8] Il ripristino dei dati o degli strumenti elettronici in caso di distruzione o danneggiamento (19.5 allegato B codice) è previsto (almeno) entro 7 giorni dall'evento dannoso (art. 23 allegato B codice). I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (art. 22 All. B "codice"); appena terminate le operazioni, i supporti di back-up su cui sono memorizzati i dati vengono custoditi al fine di evitare accessi non autorizzati e trattamenti non consentiti (art. 21 All. B "codice").

di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali (19.6 all. B codice);

- **Dati personali affidati in conformità al codice, all'esterno della struttura del titolare**: contiene l'elenco dei trattamenti che il titolare assegna all'esterno della struttura[9];
- **Tutela dei dati personali idonei rilevare eventuali dati sensibili o giudiziari**: vengono specificate le misure necessarie a garantire l'integrità e la disponibilità dei dati (19.4 all. B codice).

Devono essere allegate: Lettere di Informativa ed eventuali Lettere di Incarico (esempi indicativi sono riportati negli allegati 1 e 2 di questo articolo).

Data la complessità della materia affrontata e le peculiarità che presenta il trattamento dei dati per ciascun libero professionista, studio associato o società le informazioni e le indicazioni presenti in questo articolo non possono essere che generiche e costituiscono solo una possibile linea di guida per attuare una efficace strategia per la sicurezza. Pertanto risulta opportuno che il titolare del trattamento o un esperto di sua fiducia effettui un'analisi specifica del sistema informativo per la redazione del Documento Programmatico sulla Sicurezza e la definizione delle strategie di sicurezza e delle conseguenti policy che tutti i dipendenti, collaboratori, fornitori e partner devono seguire.

[9] Il titolare del trattamento dei dati deve stabilire i criteri da adottare per garantire l'adozione delle misure minime di sicurezza nel caso in caso il trattamento dei dati personali venga affidato all'esterno della struttura (19.7 allegato B codice).

ALLEGATO 1. INFORMATIVA AL CLIENTE
INFORMATIVA AI SENSI DELL'ART. 13 D. LGS. 196/2003

Gentile Cliente,
ai sensi dell'art. 13 D. Lgs. 196/2003 (di seguito T.U.), ed in relazione ai dati personali di cui lo studio entrerà in possesso, La informiamo di quanto segue:

1. Finalità del trattamento dei dati.
II trattamento è finalizzato unicamente alla corretta e completa esecuzione dell'incarico professionale ricevuto.
2. Modalità del trattamento dei dati
   a) II trattamento è realizzato per mezzo delle operazioni o complesso di operazioni indicate all'art. 4 comma 1 lett. a) T.U.: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione dei dati.
   b) Le operazioni possono essere svolte con o senza l'ausilio di strumenti elettronici o comunque automatizzati.
   c) II trattamento è svolto dal titolare e/o dagli incaricati del trattamento.
3. Conferimento dei dati.
II conferimento di dati personali comuni, sensibili e giudiziari è strettamente necessario ai fini dello svolgimento delle attività di cui al punto 1.
4. Rifiuto di conferimento dei dati.
L'eventuale rifiuto da parte dell'interessato di conferire dati personali nel caso di cui al punto 3 comporta l'impossibilità di adempiere alle attività di cui al punto 1.
5. Comunicazione dei dati.
I dati personali possono venire a conoscenza degli incaricati del trattamento e possono essere comunicati per le finalità di cui al punto 1 a collaboratori esterni, e, in genere, a tutti quei soggetti cui la comunicazione sia necessaria per il corretto adempimento delle finalità indicate nel punto 1.
6. Diffusione dei dati.
I dati personali non sono soggetti a diffusione.
7. Trasferimento dei dati all'estero.
I dati personali possono essere trasferiti verso Paesi dell'Unione Europea e verso Paesi terzi rispetto all'Unione Europea nell'ambito delle finalità di cui al punto 1.
8. Diritti dell'interessato.
L'art. 7 T.U. conferisce all'interessato l'esercizio di specifici diritti, tra cui quello di ottenere dal titolare la conferma dell'esistenza o meno di propri dati personali e la loro messa a disposizione in forma intelligibile; l'interessato ha diritto di avere conoscenza dell'origine dei dati, della finalità e delle modalità del trattamento, della logica applicata al trattamento, degli estremi identificativi del titolare e dei soggetti cui i dati possono essere comunicati; l'interessato ha inoltre diritto di ottenere l'aggiornamento, la rettificazione e l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione della legge; il titolare ha il diritto di opporsi, per motivi legittimi, al trattamento dei dati.
9. Titolare del trattamento.
Titolare del trattamento è _____ (indicare la persona fisica, l'associazione professionale o la società) con sede in _____
Responsabile del trattamento è il sig./dott.: _____ (da indicare se nominato).
Per ricevuta comunicazione

Data: _____ Firma: _____

ALLEGATO 2.
LETTERA DI INCARICO

Il sottoscritto _____ in qualità di Titolare/Responsabile del trattamento dei dati dello Studio/Società_____ sito in _____
INCARICA
il Dr./sig./la sig.ra _____nato/a a _____ il _____ al trattamento dei dati (personali / sensibili / giudiziari : specificare anche con i codici del d.p.s.) nell'ambito delle funzioni di _____ che è chiamato/a a svolgere presso questo Studio/Società. A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;

- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare/Responsabile in generale ed elencate nel d.p.s.

Per ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
a) divieto di comunicazione o diffusione dei dati senza la preventiva autorizzazione del Titolare/Responsabile;
b) l'accesso ai dati è autorizzato limitatamente all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
c) la fase di trattamento dei dati dovrà essere preceduta dalla informativa al cliente in forma scritta e dal consenso di quest'ultimo al trattamento nei casi previsti dalla legge;
d) in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
e) le proprie credenziali di autenticazione sono strettamente personali e devono rimanere riservate. Tali credenziali sono elencate nel documento programmatico sulla sicurezza dello Studio/Società e univocamente associate all'incaricato al quale sono state fornite.
Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.
Qualsiasi altra istruzione può essere fornita dal Titolare che provvede anche alla formazione degli incaricati.
Per ogni altra misura qui non prevista si fa riferimento al documento programmatico sulla sicurezza adottato dallo Studio/Società.

TRATTAMENTO CONSENTITO
a) raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati; b) qualsiasi accesso e trattamento espressamente previsto dal profilo di autorizzazione associato e descritto nel d.p.s.; c) qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.
Data _____ L'incaricato