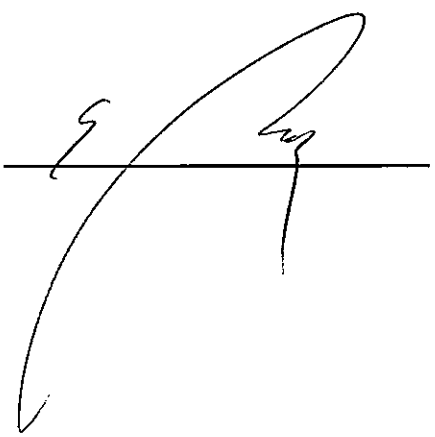
DOCUMENTO RIASSUNTIVO DEGLI ADEMPIMENTI LEGATI ALLA TUTELA DELLA PRIVACY

(aggiornato al 01 maggio 2014)

Il Responsabile del Trattamento dei Dati: _____



Applicazione delle misure minime di sicurezza per la salvaguardia dei dati oggetto dei processi elaborativi

Attuazione del d. lgs. 196 del 30 giugno 2003

1.0 Introduzione e descrizione dell'attività

Il presente Documento viene redatto come riassuntivo di tutte le misure e gli adempimenti che devono essere adottati in via preventiva da tutti coloro che trattano dati personali, conformemente a quanto previsto dal Codice in materia di dati personali (decreto legge n. 196 del 30 giugno 2003). Inoltre costituisce un valido strumento per la adozione delle misure idonee previste dall'art. 31 dello stesso Codice e dal Disciplinare tecnico in materia di misure minime di sicurezza. Grazie alle indicazioni riportate in questo documento è possibile ridurre al minimo i rischi di distruzione e di perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.
Inoltre esso fornisce una valutazione sui criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati a misure di sicurezza nonché sui criteri adottati per assicurare l'integrità dei dati; esso riguarda il trattamento di tutti i dati personali:

- sensibili
- giudiziari
- comuni,

e si applica al trattamento di tutti i dati personali per mezzo di:

- strumenti elettronici di elaborazione
- altri strumenti di elaborazione (es. cartacei, audio/video, ecc.).

Vista l'attività svolta dall'Ordine degli Ingegneri della Provincia dell'Aquila, attività che si concretizza nell'espletamento di procedure di servizio e consulenza per gli ingegneri iscritti, con conseguente necessità di raccolta ed elaborazione dei dati necessari a svolgere il lavoro in oggetto, si rende necessario analizzare i rischi connessi allo svolgimento dell'attività stessa sia nei riguardi dei dati che della struttura, nonché individuare per iscritto le procedure interne atte a salvaguardare i dati, gli accessi indesiderati ai dati stessi e le persone delegate al trattamento ed alla salvaguardia degli stessi.
La sede dell'Ordine degli Ingegneri della Provincia dell'Aquila è ora ubicata in Via Saragat, 32 a L'Aquila in un immobile di proprietà.

1.1 Dati trattati

L'Ordine degli Ingegneri della Provincia dell'Aquila tratta i seguenti dati:

- dati comuni degli iscritti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali;
- dati comuni del personale dipendente, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria;
- dati comuni degli iscritti, dagli stessi forniti per l'espletamento delle attività connesse alla realizzazione di quanto previsto dallo statuto dell'Ordine, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati comuni di terzi, forniti dagli iscritti per l'espletamento delle funzioni dell'ordine, o necessari a fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o

per atti giudiziari;
- dati comuni di committenti esterni, da loro forniti per l'espletamento di compiti legati alla necessità di individuazione di fonti interne all'ordine (es. per la creazione di terne di collaudatori, ...)
- dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria;
- dati sensibili del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti ai rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o l'adesione ad organizzazioni sindacali;
- dati sensibili degli iscritto, dagli stessi forniti per l'espletamento delle funzioni dell'Ordine.

2.0 Analisi dei rischi

Per i dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali), i dati comuni degli iscritti (dagli stessi forniti per l'espletamento dei contratti con la società, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi), i dati comuni di terzi (forniti dagli iscritti per l'espletamento di quanto previsto, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari), i dati comuni forniti da committenti esterni, i dati comuni dei fornitori (concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali), ed i dati comuni degli iscritti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali, il rischio legato alla loro gestione può definirsi basso.

Per i dati sensibili del personale dipendente, il rischio legato alla loro gestione è da definirsi altrettanto basso visto anche che l'elaborazione specifica di tali dati è affidata all'esterno, presso un consulente di provata sicurezza ed affidabilità in regola con le norme sulla privacy dettate dal d. lgs. 196/2003.

Per quanto riguarda gli strumenti elettronici, possono verificarsi malfunzionamenti, guasti, eventi naturali, intromissioni di esterni.

Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori, virus, intercettazioni dei dati.

Per quanto riguarda le aree ed i locali: possono essere colpiti da eventi naturali o accessi di terzi non autorizzati.

Per quanto riguarda i supporti di memorizzazione, il rischio di deterioramento dei dati da essi portati può essere ritenuto basso, attesi i frequenti back up ed il fatto che essi sono conservati in armadi metallici, così come i dischi di installazione dei programmi software adottati. Non vi sono elaboratori non in rete, non vi sono elaboratori non in rete e connessi ad internet, per cui nessun giudizio di rischio deve essere dato su detti strumenti.

Atteso, infine, che gli incaricati al trattamento dei dati oltre al responsabile sono da ritenersi persone qualificate ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio afferente la riservatezza, o la distrazione, o l'incuria degli stessi, può essere definito basso.

Inoltre i dati, quanto comuni che sensibili, non paiono essere di particolare interesse per terzi.

3.0 Definizione dei ruoli del personale

Il titolare dei dati è l'Ordine degli Ingegneri della Provincia dell'Aquila nel suo essere persona giuridica; il Responsabile del Trattamento dei dati è l'ing. Elio Masciovecchio, presidente nominato per elezione della struttura stessa; a lui competono le decisioni strategiche di fondo sulle modalità e sulle finalità della raccolta dei dati, dell'organizzazione del trattamento e delle risorse da dedicare per la salvaguardia della sicurezza.
È autorizzato al trattamento dei dati il personale riportato nell'allegato elenco, oltre al responsabile stesso.

Per quel che concerne l'utilizzo dei personal computer disponibili all'interno della struttura, si evidenzia che gli incaricati possono utilizzare tutti i programmi in uso ovviamente accedendo ai diversi personal computer ognuno con le proprie credenziali di autenticazione.

I locali in cui si svolge l'attività sono forniti di sistema di allarme.
Non è consentito l'accesso dei clienti nelle zone nelle quali si potrebbero verificare danneggiamenti ai dati ivi custoditi sia in formato elettronico che cartaceo.

4.0 Descrizione degli archivi e delle procedure

4.1 Archivi cartacei
Gli archivi cartacei sono contenuti in faldoni e raccoglitori divisi per tipologia e conservati in armadi chiusi e/o mobili a ripiani; gli archivi cartacei sono conservati in vari uffici e nei corridoi di passaggio.
Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione contabile degli associati) sono ubicate in modo tale che il responsabile o qualcuno degli incaricati possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.

4.2 Archivi elettronici
La rete elaborativa dell'Ordine degli Ingegneri della Provincia dell'Aquila è formata da personal computer collegati in rete tra di loro; il collegamento ad Internet può avvenire da tutti i PC.
I programmi utilizzati all'interno della società sono quelli necessari per lo svolgimento di procedure di office automation ed un programma gestionale sviluppato da terze parti e specifico per la gestione dell'Ordine.
L'ubicazione di stampanti ed apparecchi telefax tradizionali non consente ad estranei di leggere o eventualmente asportare documenti non ancora prelevati dal personale.

4.3 Criteri e procedure per assicurare l'integrità dei dati
Di seguito si illustrano le norme applicate per garantire la sicurezza e l'integrità dei dati per:

- **computer e supporti informatici**

I software per la gestione dell'Albo Professionale e della Contabilità sono ospitati in un data center sito presso la sede stessa, di cui si specificano di seguito le caratteristiche.

Linea elettrica dedicata
Gli apparati della nuova infrastruttura realizzata risiedono all'interno di una stanza ad accesso limitato e costantemente climatizzata; la ditta Future System ha derivato una linea elettrica dedicata direttamente dal quadro.

Armadi Rack
Tutti gli apparati infrastrutturali sono installati all'interno di due armadi rack, uno bianco più piccolo contenente soltanto apparati di rete e un altro nero, più capiente, contenente i server e il firewall.
L'armadio bianco era già installato in sede, mentre l'armadio nero è stato acquistato tramite la ditta Future System ed installato nel mese di luglio 2012.
Gli armadi sono chiusi a chiave e le chiavi sono riposte all'interno della cassetta di sicurezza presso la segreteria dell'Ordine.
L'armadio nero è ventilato ed ha un sensore interno di temperatura.

UPS
Ciascun armadio ha un gruppo di continuità elettrica nuovo (UPS) per garantire il funzionamento degli apparati anche in assenza di corrente elettrica e per evitare sbalzi di tensione. L'armadio bianco ha un gruppo APC più piccolo, l'armadio nero ha un gruppo DELL che supporta un carico più elevato e viene monitorato da un software all'interno del server.

Server
Nell'armadio nero è posizionato un nuovo server DELL, dedicato all'infrastruttura software, che ha tutte componenti fondamentali ridondate (2 CPU, 2 alimentatori, 2 dischi in mirroring (RAID 1) ed ha una maschera di protezione fisica con chiave.
Nell'armadio nero è ospitato anche il precedente mini-server HP che adesso svolge soltanto funzioni di backup e ospita il vecchio sito web dell'Ordine.

Firewall e altri apparati di rete
Nell'armadio nero è stato posizionato uno switch gigabit per gestire la rete dei server e un firewall hardware CISCO Serie RV, che protegge tutta la LAN dagli accessi esterni mediante regole configurabili.
La nuova rete realizzata è Dual Stack in quanto supporta i protocolli IPv4 e IPv6.
Gli accessi dall'esterno sono possibili soltanto tramite connessioni sicure in VPN.

NAS
Nell'armadio c'è anche un server NAS Lacie 2Big Network per gestire i backup periodici dei documenti. Il NAS contiene due dischi in configurazione RAID-1 (mirroring) da 2TB. I software di backup acquistati (Lacie Backup e Uranium Backup) salvano periodicamente i dati dei vari server sul NAS, inviando anche per email un report di riepilogo con l'esito dei salvataggi effettuati.

Backup online
Le banche dati di contabilità e della gestione dell'Albo sono settimanalmente salvati su un server online di Memopal, esterno alla sede dell'Ordine, per garantire il disaster recovery in quanto il servizio memorizza i dati su un file-system RAID-5 geografico cifrato.

Rete WiFi
Presso al sede sono attualmente disponibili tre reti wireless differenti e logicamente separate:

1. Rete wifi per i dipendenti, a 2.4GHz e 5 GHz, senza restrizioni;
2. Rete wifi per gli ospiti della sala riunioni (2.4 GHz);
3. Rete wifi per il video proiettore ai monitor della sala riunioni (2.4 GHz).

Le reti sono indipendenti e dotate di cifratura e protezione con protocollo WPA2. La rete WiFi è Dual Stack, cioè supporta IPv4 e IPv6.

Directory
Tutta la rete informatica è gestita tramite un dominio centralizzato di Microsoft Active Directory e denominato ORDINGAQ. Il sistema fornisce accesso mediante single-sign-on su ogni postazione con account personali, gruppi e criteri di autorizzazione delle risorse in rete.
Il dominio supporta della policy centralizzate (GPO) per la gestione dei criteri di protezione, come ad esempio la password, che deve rispettare i criteri minimi di sicurezza e si deve modificare con cadenza almeno semestrale.
I server controller gestiscono anche i servizi DNS, DHCP, DHCPv6, Print Server, SMTP Server.

Antivirus
Sui server e su tutte le postazioni client è stato installato il software antivirus Symantec, che si aggiorna automaticamente in rete ed offre protezione antivirus e antispyware.

· **supporti cartacei**: relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nei seguenti:

- qualsiasi documento che venga consegnato all'Ordine va inserito, quando personale, in apposite cartelline non trasparenti;
- qualsiasi documento che la società consegni aiscritti o fornitori va inserito in apposite buste o cartelline non trasparenti.

Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non contiene alcun dato (praticamente il primo foglio funge da copertina). In generale nessun dato riportato su carta deve essere visibile da personale esterno alla struttura.

Le copie dei telefax inviati mediante apparecchio tradizionale sono subito riconsegnate a colui che ha eseguito la trasmissione ed archiviate nelle relative cartelle.
Per ciò che concerne le trasmissioni del telefax, nella copertina del messaggio è inserita la seguente dicitura:
"Qualora questo messaggio fosse da Voi ricevuto per errore vogliate cortesemente darcene notizia a mezzo telefax od e-mail e distruggere il messaggio ricevuto erroneamente. Quanto precede ai fini del rispetto del D. Lgs. 196/2003 sulla tutela dei dati personali."
La stessa dicitura viene riportata anche in calce alle e-mail inviate.
Il materiale cartaceo non più utilizzabile, ridotto in pezzi e destinato allo smaltimento dei rifiuti sarà riposto negli appositi sacchi di plastica e detti sacchi, chiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, verranno giornalmente eliminati.

. **accesso ai locali:** il rischio di accesso ai locali della società può essere definito basso, vista l'esistenza di portone d'ingresso al palazzo e portoncino con chiusura di sicurezza.
Il rischio di accesso ai singoli strumenti da parte di persone non autorizzate durante l'orario di lavoro può essere definito basso, essendo controllato l'accesso ai locali ed essendo protetti da password gli strumenti stessi.
Per quanto riguarda gli strumenti elettronici, il rischio può essere definito basso, essendo state adottate dallo studio le misure di sicurezza, tendenti a ridurre il rischio gravante sui dati e

derivante dalla gestione di detti strumenti.

5.0 Criteri tecnici e organizzativi per la protezione dei locali e degli archivi cartacei

Essendo l'Ordine degli Ingegneri della Provincia dell'Aquila una struttura che non esercita attività commerciale ma solo attività di servizio e consulenza verso i propri iscritti, non tutti i suoi locali di lavoro sono liberamente accessibili al pubblico; infatti i locali utilizzati come archivio e la sona riservata alla segreteria non sono accessibili a esterni.
L'eventuale presenza di personale di pulizia avverrà solo in presenza di uno degli incaricati.
Si è disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli contenenti dati personali. I fascicoli vanno conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti.
Le comunicazioni a mezzo posta, o a mezzo telefax, dovranno essere tempestivamente smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato e consegnato all'interessato.

6.0 Criteri tecnici e organizzativi per la protezione dei dati elettronici

1. Tutto il personale incaricato del trattamento dei dati è dotato di UserID e Password individuale per accedere all'elaboratore a lui assegnato. La password personale è almeno di 8 (otto) caratteri o, nel caso il sistema non preveda tale lunghezza, tale password deve essere lunga il numero massimo dei caratteri ammissibili; tale password deve essere variata almeno ogni sei mesi.
2. Tutte le stazioni personal computer in cui è possibile inserire dati da supporti esterni sono dotate di software antivirus, software che l'amministratore di sistema manterrà costantemente aggiornato; i PC collegabili ad Internet sono anche dotati di un programma di firewall avente lo scopo di impedire intercettazioni di dati via Web e accessi non desiderati.
3. Tutte le stazioni personal computer sono dotate di password applicata al bios che ha lo scopo di non permettere l'inserimento di supporti di partenza nel computer.
4. Tutte le stazioni personal computer sono dotate di password all'avvio del sistema operativo.
5. Tutto il personale incaricato del trattamento dovrà aver cura di spegnere la stazione personal computer sul quale ha lavorato al termine dell'attività e comunque di attivare lo "screen saver con propria password" nel caso la lasci incustodita anche per brevi periodi; si consiglia di attivare lo screen saver dopo 1 minuto di assenza e comunque di farlo partire dopo non oltre 5 minuti dal mancato utilizzo del computer.

Copia di tutte le password utilizzate da ogni incaricato saranno scritte da ognuno su un apposito modulo che verrà messo all'interno di una busta successivamente chiusa, busta che sarà custodita in apposito contenitore.

Alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei allo studio, viene dato incarico scritto con richiesta di specificazione dei nominativi delle persone che accedono ed espresso invito a limitarsi alle sole attività pertinenti alla prestazione per cui accedono.

Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici, verranno seguiti i seguenti passi logico/operativi:

- avvertire dell'avvenuto danneggiamento il titolare del trattamento dei dati e l'incaricato che ha in custodia i cd di backup nonché i cd contenenti i vari software installati sugli strumenti elettronici;
- chiedere immediatamente l'intervento di un tecnico manutentore sollecitandone al più presto l'assistenza; ci si rivolgerà sempre a tecnici di provata esperienza e fiducia;
- dopo aver reinstallato tutti i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, si provvederà a ricaricare tutti i dati contenuti nei supporti di backup;
- si provvederà all'aggiornamento dei sistemi operativi e dei programmi utilizzati una volta reinstallati;
- verrà dato incarico al tecnico manutentore di suggerire ogni altra misura;
- in ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;
- al fine di evitare eventi di perdita e di danneggiamento degli strumenti elettronici e dei dati in essi contenuti, si prevede che per due volte all'anno sia effettuata manutenzione in modo adeguato da un tecnico incaricato.

7.0 Diritti dell'interessato

7.1 Diritto di accesso ai dati personali – art. 7 d.l. 196/2003

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.

7.2 Esercizio dei diritti – art. 8 d.l. 196/2003

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:

a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;

b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;

c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;

f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;

g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;

h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

7.3 Modalità di esercizio – art. 9 d.l. 196/2003

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.
3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.
5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

7.4 Riscontro all'interessato – art. 10 d.l. 196/2003
1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.
2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.
3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.
4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.
5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.
6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.
7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.
8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al

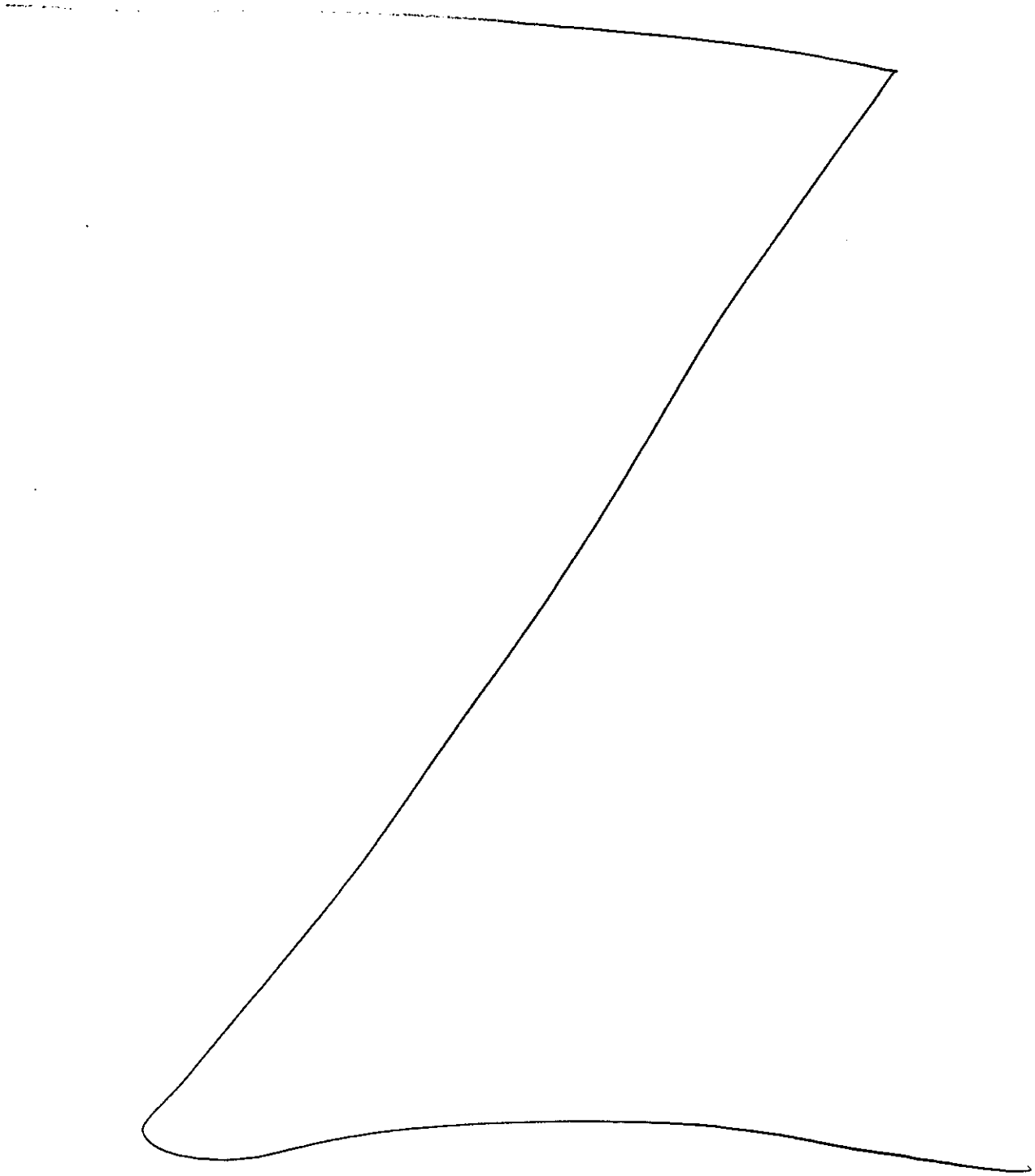
caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.
9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

8.0 Conclusioni

Si ribadisce che il presente documento scaturisce da una analisi di valutazione dei rischi alla data attuale e che si dovrà provvedere all'aggiornamento del presente documento nel caso di sostituzione di attrezzature o di cambiamenti nella disposizione degli spazi di lavoro o degli incaricati.
La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali.
Inoltre essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile o giudiziaria.
La formazione è fatta dal Responsabile del trattamento dei dati o da un suo incaricato.
Nel caso in cui il trattamento dei dati venga affidato, per qualsiasi motivo, a soggetti esterni che li trattino con strumenti elettronici, per avere la garanzia che essi adottino le misure minime di sicurezza, si esigerà dagli stessi una dichiarazione nella quale attestino di aver adottato le misure minime previste dal d. lgs. 196/2003.
Gli incaricati del trattamento sono stati debitamente informati circa il contenuto del presente documento e sono obbligati ad uniformarsi allo stesso mentre il responsabile del trattamento è obbligato a vigilare sull'osservanza delle disposizioni stesse da parte degli incaricati.

L'Aquila, li 01.05.2014

Il Responsabile del Trattamento



ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI COMUNI, SENSIBILI E/O GIUDIZIARI

In ottemperanza alle disposizioni del Codice in materia di protezione dei dati personali (D.Lgs 196/03) ed in relazione alle attività svolte nell'ambito della Struttura in oggetto, l'"*Incaricato*", dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni ed ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal "Responsabile del trattamento".
I dati personali devono essere trattati:

a) in osservanza dei criteri di riservatezza;

b) in modo lecito e secondo correttezza;

c) per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;

d) nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure minime di sicurezza (di cui agli artt. 33 – 36 ed allegato B del citato Dlgs. 196/03) sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:
1. senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);
2. con strumenti elettronici (PC ed elaboratori).

1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

1.1 CUSTODIA

- □I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave).
- □□I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- □□I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

1.2 COMUNICAZIONE

L'utilizzo dei dati personali deve avvenire in base al principio del *"need to know"* e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno e comunque a soggetti terzi se non previa autorizzazione.

1.3 DISTRUZIONE

- Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
- □□I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

1.4 ULTERIORI ISTRUZIONI IN CASO DI TRATTAMENTO DI DATI SENSIBILI E/O GIUDIZIARI

- I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi dagli Incaricati in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.
- □□L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.
- Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

2. TRATTAMENTI CON STRUMENTI ELETTRONICI

2.1 GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

La legge prevede che l'accesso alle procedure informatiche che trattano dati personali sia consentito agli Incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. smart card) o in una caratteristica biometrica. Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni.

- Le user-id individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se Incaricati del trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Responsabile del trattamento.
- □□Gli strumenti di autenticazione (ad esempio le password) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Incaricati del trattamento).
- □Le password devono essere sostituite, a cura del singolo Incaricato, al primo utilizzo e successivamente almeno ogni sei mesi.
- Le password devono essere composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Le password non devono contenere riferimenti agevolmente riconducibili all'Incaricato (es. nomi di familiari) e devono essere scelte nel rispetto della normativa generale sulla costruzione ed utilizzo delle password (vedi successivo punto 3.).

2.2 PROTEZIONE DEL PC E DEI DATI

- □□Tutti i PC devono essere dotati di password e, ove possibile, va impostata anche la password di BIOS.

- □Le password di accesso ai PC contenenti dati personali, nonché le eventuali password per l'accesso ai singoli file contenenti tali dati devono essere consegnate in busta chiusa al Custode delle password.
- □□Tutti i PC devono essere dotati di software antivirus aggiornato costantemente e con la funzione "Monitor" attiva.
- Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalle strutture di appartenenza. Sono vietati i software scaricati da Internet o acquisiti autonomamente.
- □Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password.
- □□Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.
- Deve essere effettuato, con cadenza almeno settimanale un salvataggio di back-up di eventuali dati personali presenti unicamente sul PC personale. I supporti di memoria utilizzati per il back-up devono essere trattati secondo le regole definite al punto "Trattamento senza l'ausilio di strumenti elettronici".

2.3 CANCELLAZIONE DEI DATI DAI PC

I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.

2.4 ULTERIORI ISTRUZIONI IN CASO DI TRATTAMENTI DI DATI SENSIBILI E/O GIUDIZIARI

- □Le password di accesso alle procedure informatiche che trattano dati sensibili e/o giudiziari devono essere sostituite, da parte del singolo incaricato, almeno ogni tre mesi.
- □□L'installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi per elaboratori deve essere effettuato almeno semestralmente.

3. ISTRUZIONI DI CARATTERE GENERALE

Come scegliere e usare la password (Normativa sulla costruzione ed utilizzo delle password)

- Usare almeno 8 caratteri, o nel caso in cui lo strumento elettronico non lo permetta, usare un numero di caratteri pari al massimo consentito.
- □□Usare lettere, numeri e almeno un carattere tra . ; $! @ - > <
- □Non utilizzare date di nascita, nomi o cognomi propri o di parenti
- □□Non sceglierla uguale alla matricola o alla user-id
- □□Custodirla sempre in un luogo sicuro e non accessibile a terzi
- □□Non divulgarla a terzi
- □□Non condividerla con altri utenti

Come comportarsi in presenza di ospiti o di personale di servizio

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- □□Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del PC .
- Non rivelare o fare digitare le password dal personale di assistenza tecnica.□□ Non rivelare le password al telefono né inviarla via fax - nessuno è autorizzato a chiederle.
- □□Segnalare qualsiasi anomalia o stranezza al Responsabile.

Come gestire la posta elettronica

- Non aprire messaggi con allegati di cui non si conoscono l'origine, possono contenere virus in grado di cancellare i dati sul PC.
- □□Evitare di aprire filmati e presentazioni non attinenti l'attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul vostro PC.

Come usare correttamente Internet

- Evitare di scaricare dalla rete file e software di uso non direttamente riferibile all'attività di lavoro, in quanto questo può essere pericoloso. I software necessari all'attività lavorativa vanno richiesti alle persone competenti per incarico.
- □□Usare Internet solo per lavoro, i siti web spesso nascondono insidie per i visitatori meno esperti.
- □□Non leggere le caselle personali esterne via webmail in quanto alcuni provider esterni non proteggono dai virus.

4. SANZIONI PER INOSSERVANZA DELLE NORME

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy, l'inosservanza delle quali da parte dell'Incaricato può comportare sanzioni anche di natura penale a suo carico.