DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Codice in materia di protezione dei dati personali
Art. 34 e allegato B, del D.Lgs. 30/06/2003, n. 196

Il Titolare del Trattamento

Cicconi Giuliano

Ediz	Rev.	Data revisione	Descrizione
2	0	23/03/2012	Aggiornamento
	1	29/03/2013	Aggiornamento
	2	27/03/2014	Aggiornamento
	3	24/03/2015	Aggiornamento
	4	24/05/2016	Aggiornamento
	5		

INDICE

1 Introduzione e riferimenti

1.1 Scopo

Scopo del presente documento è garantire la conformità dei trattamenti di dati personali a quanto previsto dal Codice in materia di protezione dei dati personali (D.lgs. n. 196 del 30 giugno 2003) e garantire l'adozione delle misure previste dall'Art. 31, dall'Art.33, dall'Art. 34 e dall'Art. 35 e dal Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003).

1.2 Campo di applicazione

Il Documento Programmatico sulla Sicurezza (**DPS**) definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il **DPS** riguarda il trattamento di tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il **DPS** si applica al trattamento di tutti i dati personali effettuato per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il **DPS** deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

1.3 Riferimenti Normativi

Il presente documento è stato redatto in conformità al D.Lgs. n. 196 del 30 giugno 2003 (in particolare al disciplinare tecnico in materia di misure minime di sicurezza - allegato B), tenendo conto delle indicazioni contenute nella "Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)".

1.4 Termini e Definizioni

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

Dato personale: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato;

Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

Interessato: la persona fisica cui si riferiscono i dati personali;

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Banca dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

2 Anagrafica dell'azienda

Ragione sociale	CIMAR Soc Coop
Sede Legale	Via Timante, 32 – 00124 Roma
Legale rappresentante	Sig. Cicconi Giuliano
Tipo di attività svolta	Lavori di edilizia, manutenzione impianti, pulizie, disinfestazione e derattizzazione
N° dipendenti	80
P.IVA	05736491001
Telefono	06/50913515
Fax	06/50931668
E-mail	segreteria@cimarscarl.it

3 Riepilogo figure aziendali

In questa sezione sono indicati gli estremi identificativi del Titolare del trattamento, nonché, se designati, degli eventuali Responsabili.

L'organizzazione ha deciso di non nominare i responsabili per il trattamento.

Figura	Nominativo
Titolare del trattamento	Cicconi Giuliano
Responsabile del trattamento	N.N.
Incaricato delle copie di sicurezza e del ripristino delle banche dati	Stefano Arzillo
Incaricato della gestione e manutenzione degli strumenti elettronici	Stefano Arzillo

4 Riepilogo delle sedi della società incaricate del trattamento

Sede	Indirizzo
Sede unica	Via Timante, 32 – 00124 Roma

5 Riepilogo strutture incaricate del trattamento

In questa sezione sono riportate le strutture interne ed esterne incaricate del trattamento dei dati.

Struttura interna	Tipo di dati
Amministrazione	Dati anagrafici e contabili fornitori e clienti
Ufficio del personale	Dati anagrafici e contabili personale dipendente

Struttura esterna	Tipo di dati
• **Studio Anellucci** (Commercialista)	Dati anagrafici e contabili di clienti e fornitori
• **Dott.ssa Nada Romani** (Consulente del lavoro)	Dati anagrafici e contabili del personale dipendente
• **Basic S.r.l.** (Soc. di consulenza per gli adempimenti del D. Lgs 81/08)	Dati anagrafici del personale dipendente
• **Dott. Cristiano De Arcangelis** (Medico del lavoro)	Dati anagrafici e sanitari del personale dipendente

6 Elenco dei trattamenti di dati personali

6.1 Informazioni essenziali

In questa sezione sono censiti i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

Tabella 1.

Descrizione sintetica del trattamento		Natura dei dati trattati			Struttura interna di riferimento	Strutture esterne che concorrono al trattamento	Descrizione degli strumenti utilizzati	Eventuale Banca Dati	Ubicazione fisica dei supporti di memorizzazione
Finalità perseguita o attività svolta	Categorie di interessati	C	S	G					
Gestione acquisti	Fornitori	X			Amministrazione	Commercialista	PC in LAN con collegamento internet	Archivio informatico – Software gestionale	Sede unica
Gestione clienti	Clienti	X			Amministrazione	Commercialista	PC in LAN con collegamento internet	Archivio informatico – Software gestionale	Sede unica
Gestione del Personale	Dipendenti	X	X		Ufficio del personale	Consulente del lavoro	PC in LAN con collegamento internet	Archivio informatico – Software gestionale	Sede unica
D.Lgs. 81/08 (sicurezza e salute dei lavoratori)	Dipendenti	X			Ufficio del personale	Basic S.r.l.	PC in LAN con collegamento internet	Archivio informatico	Sede unica
Sorveglianza sanitaria ai sensi dell'Art. 41 del D.Lgs. 81/2008	Dipendenti	X	X		Ufficio del personale	Dott. Cristiano De Arcangelis			Sede unica

6.2 Distribuzione dei compiti e delle responsabilità

In questa sezione sono descritte sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.

Tabella 2.

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Amministrazione	Gestione dati anagrafici e contabili dei clienti e fornitori (es. per fatturazione)	Acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc)
Ufficio del personale	Gestione dati anagrafici e contabili dei dipendenti (es. assunzioni e buste paga, ferie, permessi, sicurezza,sul lavoro ecc)	Acquisizione e caricamento dei dati, consultazione, comunicazione a terzi

Nell'allegato **INC** sono riportati i nominativi degli incaricati al trattamento suddivisi per struttura/funzione.

7 Analisi dei rischi che incombono sui dati e misure in essere e da adottare

In questa sezione sono indicati i principali eventi potenzialmente dannosi per la sicurezza dei dati nonché la valutazione delle possibili conseguenze e la gravità in relazione al contesto fisico–ambientale di riferimento e agli strumenti elettronici utilizzati e le misure in essere e quelle da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Nelle tabelle seguenti sono riportati i risultati di tali attività.

Tabella 3.

Rischi		Impatto sulla sicurezza				Misure	Trattamenti interessati	In essere	Struttura o persone addette all'adozione
		Si/No	Descrizione	Valutazione del rischio					
COMPORTAMENTI DEGLI OPERATORI	**Sottrazione di credenziali di autenticazione**	SI	Fa riferimento al caso in cui le credenziali di autenticazione siano acquisite e utilizzate indebitamente da terzi. Ciò consente l'accesso non autorizzato ai dati e espone a rischi ulteriori (come il danneggiamento), se si aggiungono altri eventi.	Probabilità	Bassa	Formazione del personale sulla idonea scelta e conservazione delle credenziali di autenticazione	Trattamenti con strumenti elettronici	X	Incaricati del trattamento
				Entità	Bassa				
				Rischio	**Basso**				
	Carenza di consapevolezza, disattenzione o incuria	SI	Fa riferimento al caso in cui, a causa di un utilizzo disattento degli strumenti, i dati vengano alterati o corrotti in modo irrecuperabile, ovvero vengano cancellati.	Probabilità	Media	Formazione del personale	Trattamenti con strumenti elettronici	X	Titolare del trattamento
				Entità	Media				
				Rischio	**Medio**				
	Comportamenti sleali o fraudolenti	SI	Fa riferimento alla possibilità di sfruttare, nell'ottica di un comportamento sleale o fraudolento, eventuali debolezze nel sistema di sicurezza dei programmi o della rete. Questo può portare non solo all'accesso non autorizzato ai dati, ma anche ad un danneggiamento dei dati stessi.	Probabilità	Bassa	Utilizzo delle credenziali di autenticazione. Aggiornamento costante dei sistemi di sicurezza (antivirus, firewall, patch, ecc.)	Trattamenti con strumenti elettronici	X	Titolare del trattamento
				Entità	Alta				
				Rischio	**Medio**				
	Errore materiale	SI	Fa riferimento al caso in cui, a causa di un errore commesso in modo inconsapevole durante l'utilizzo di software o di apparecchiature elettroniche, i dati vengano danneggiati, corrotti o cancellati.	Probabilità	Media	Formazione del personale	Trattamenti con strumenti elettronici	X	Titolare del trattamento
				Entità	Media				
				Rischio	**Medio**				

Tabella 4.

Rischi		Impatto sulla sicurezza				Misure	Trattamenti interessati	In essere	Struttura o persone addette all'adozione
		Si/No	Descrizione	Valutazione del rischio					
EVENTI RELATIVI AGLI STRUMENTI	**Azione di virus informatici o di programmi suscettibili di recare danno**	SI	Fa riferimento all'effetto di virus informatici programmati per cancellare i dati a cui l'utente ha accesso o comunque danneggiarli, ovvero per causare la paralisi di servizi informatici che possono risultare in una indisponibilità temporanea dei dati.	Probabilità Entità **Rischio**	Bassa Media **Medio**	Installazione e aggiornamento costante di programmi antivirus, antispyware e antimalware, antispam	Trattamenti con strumenti elettronici	X	Incaricato della gestione e manutenzione degli strumenti elettronici
	Spamming o tecniche di sabotaggio	SI	Fa riferimento ad azioni di sabotaggio compiute da terzi tramite programmi appositi che, sfruttando difetti del software utilizzato per la gestione della posta elettronica o altri servizi informatici, saturano il servizio stesso di richieste fino alla paralisi parziale o totale. Questa azione risulta nella indisponibilità temporanea dei dati gestiti dal servizio che viene attaccato	Probabilità Entità **Rischio**	Bassa Media **Medio**	Installazione e aggiornamento costante di programmi antivirus, antispyware e antimalware, antispam	Trattamenti con strumenti elettronici	X	Incaricato della gestione e manutenzione degli strumenti elettronici
	Malfunzionamento, indisponibilità o degrado degli strumenti	SI	Fa riferimento alla possibilità, insita in ogni strumento (hardware o software), di rivelare difetti di funzionamento inizialmente non presenti o non evidenti. Il risultato di tale evento può essere l'indisponibilità temporanea o addirittura persistente di dati nel caso più grave, in cui cioè non sia più possibile ristabilire la situazione originaria.	Probabilità Entità **Rischio**	Bassa Alta **Medio**	Aggiornamento costante dei software e manutenzione/sostituzione dell'hardware	Trattamenti con strumenti elettronici	X	Incaricato della gestione e manutenzione degli strumenti elettronici
	Accessi esterni non autorizzati	SI	Fa riferimento al caso in cui dall'esterno vi siano intrusioni via rete, avvenute senza furto di credenziali e non dovute a semplice comportamento sleale, ma semplicemente dovute allo sfruttamento di difetti del software, per effettuare accessi non autorizzato ai dati.	Probabilità Entità **Rischio**	Bassa Media **Medio**	Installazione e aggiornamento costante di un firewall	Trattamenti con strumenti elettronici	X	Incaricato della gestione e manutenzione degli strumenti elettronici
	Intercettazione di informazioni in rete	SI	Fa riferimento a un'operazione volontaria che si basa sull'analisi e sul filtraggio dei pacchetti dati in transito sulla rete, generalmente con l'ausilio di software apposito. Il rischio è di accesso non autorizzato ai dati.	Probabilità Entità **Rischio**	Bassa Media **Medio**	Installazione e aggiornamento costante di un firewall Accesso protetto alla rete wireless	Trattamenti con strumenti elettronici	X	Incaricato della gestione e manutenzione degli strumenti elettronici

Tabella 5.

Rischi		Impatto sulla sicurezza				Misure	Trattamenti interessati	In essere	Struttura o persone addette all'adozione
		Si/No	Descrizione	Valutazione del rischio					
EVENTI RELATIVI AGLI STRUMENTI	**Ingressi non autorizzati a locali/aree ad accesso ristretto**	SI	Fa riferimento alla possibilità di accedere fisicamente a locali o reparti il cui accesso sia limitato ai soli impiegati della struttura. Il rischio è quello di accesso non autorizzato ai dati	Probabilità	Bassa	L'accesso agli uffici è consentito soltanto al personale aziendale. Videosorveglianza	Tutti	X	Titolare del trattamento
				Entità	Alta				
				Rischio	**Medio**				
	Sottrazione di strumenti contenenti dati	SI	Fa riferimento al rischio di furto di una intera postazione di lavoro o di un server, con relativa perdita dei dati in esso contenuti. Il rischio correlato è quello di accesso non autorizzato ai dati, non ché di perdita degli stessi.	Probabilità	Bassa	Sistema di allarme Utilizzo di credenziali di autenticazione	Trattamenti con strumenti elettronici	X	Titolare del trattamento Incaricato della gest. e manut. degli strumenti elettronici
				Entità	Alta				
				Rischio	**Medio**				
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	SI	Include tutti gli eventi di effetto distruttivo sui supporti fisici contenenti i dati o sulle apparecchiature. Il rischio risultante sui dati è quello di danneggiamento, indisponibilità temporanea o perdita parziale o totale.	Probabilità	Bassa	Backup su supporto rimovibile	Tutti	X	Incaricato delle copie di sicurezza delle banche dati
				Entità	Alta				
				Rischio	**Medio**				
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	SI	Si riferisce a tutti quegli eventi che, avendo impatto sui sistemi esterni e complementari agli strumenti informatici, ne inficiano la funzionalità. Ciò include impianto elettrico, climatizzazione, eccetera. Il rischio correlato è quello di danneggiamento dei dati, e di indisponibilità temporanea.	Probabilità	Bassa	Manutenzione degli impianti Protezione da sbalzi e assenza di tensione (UPS)	Trattamenti con strumenti elettronici	X	Titolare del trattamento
				Entità	Media				
				Rischio	**Basso**				
	Errori umani nella gestione della sicurezza fisica	SI	Si riferisce a ogni evento causato da errore umano nella gestione della sicurezza sugli ambienti fisici. In questa categoria ricadono porte o serrature lasciate erroneamente aperte, protezioni fisiche male installate, eccetera. Il rischio correlato va da quello di accesso non autorizzato ai dati a quello di perdita dei dati.	Probabilità	Bassa	Formazione	Trattamenti con strumenti elettronici	X	Titolare del trattamento
				Entità	Media				
				Rischio	**Basso**				

8 Criteri e modalità di ripristino della disponibilità dei dati

In questa sezione sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati.

Tabella 6.

Salvataggio e Ripristino

Banca dati/data base/archivio di dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio/ripristino	Pianificazione delle prove di ripristino
Archivio dati clienti	Back-up con cadenza settimanale su Hard Disk esterno Ripristino mediante copia da supporto di backup su posizione originaria dati previa verifica completezza dei dati.	Amministrazione	Incaricato delle copie di sicurezza delle banche dati	Semestrali
Archivio dati fornitori				
Archivio dati dipendenti				

9 Pianificazione degli interventi formativi previsti

In questa sezione sono riportate le informazioni necessarie per individuare i previsti 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 al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. Segue il quadro sintetico degli interventi formativi che si prevede di svolgere.

Tabella 7.

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Corso base privacy (formazione all'atto del conferimento dell'incarico e consegna manuale informativo)	Nuovi assunti o cambio mansione	Prima di iniziare i trattamenti

10 Trattamenti affidati all'esterno

In questa sezione è riportato il quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Tabella 8.

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Adempimenti fiscali	Dati anagrafici e contabili di clienti e fornitori	**Studio Anellucci** Commercialista	Lettera di incarico con indicazione specifica di: • trattamento dei dati ai soli fini dell'espletamento dell'incarico ricevuto; • adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
Aspetti contabili/amministrativi relativi al personale dipendente	Dati anagrafici e contabili del personale dipendente	**Dott.ssa Nada Romani** Consulente del lavoro	
Gestione degli adempimenti obbligatori previsti dal D.Lgs 81/2008 – TUSL in materia di igiene e sicurezza nei luoghi di lavoro	Dati anagrafici del personale dipendente	**Basic S.r.l.** (Soc. di consulenza per gli adempimenti del D.Lgs 81/08)	
Sorveglianza sanitaria ai sensi dell'Art. 41 del D.Lgs. 81/2008	Dati anagrafici e sanitari del personale dipendente	**Dott. Cristiano De Arcangelis** (Medico del lavoro)	

11 Trattamenti con strumenti elettronici

Nel presente paragrafo si riportano le misure adottate relativamente ai trattamenti effettuati con strumenti elettronici in base a quanto stabilito dall'allegato B del Codice in materia di protezione dei dati personali.

11.1 Istruzioni agli incaricati del trattamento

(modalità applicative delle regole di cui ai punti 4, 9, 18 e 21 dell'All. B)

Agli incaricati del trattamento dei dati effettuati con strumenti elettronici il titolare fornisce adeguate istruzioni in materia di misure di sicurezza minime attraverso le indicazioni riportate sulla lettera di incarico e manuali informativi consegnati all'atto del conferimento dell'incarico.

Nello specifico agli incaricati saranno impartite istruzioni al fine di :

- assicurare la segretezza della componente riservata della credenziale;
- la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato;
- non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- effettuare il salvataggio dei dati con frequenza almeno settimanale;
- custodire e utilizzare al meglio i supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

11.2 Sistema di autenticazione informatica

(modalità applicative delle regole di cui ai punti 1, 2, 3, 5, 6, 7, 8, 10 e 11 dell'All. B)

Per l'accesso ai sistemi informatici viene utilizzato un sistema di autenticazione basato su nome utente (username) associato ad una parola chiave (password) in modo che:

- il nome utente individui in modo univoco una sola persona, evitando che soggetti diversi utilizzino codici identici;
- la parola chiave sia conosciuta solo dalla persona che accede ai dati.

Il nome utente deve essere disattivato quando l'incaricato non ha più la qualità che rende legittimo l'utilizzo dei dati (ad esempio, in quanto non opera più all'interno dell'organizzazione).

La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato e non può essere assegnata ad altri incaricati, neppure in tempi diversi.

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Le parole chiave non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

11.3 Altre misure di sicurezza
(modalità applicative delle regole di cui ai punti 15, 16, 17, 18 dell'All. B)

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici (ad esempio *antivirus*), nonché a correggerne difetti (ad esempio *patch del Sistema Operativo*), sono effettuati mediante un sistema di aggiornamento automatico (live update) o, in assenza di tale funzionalità, almeno semestralmente.

I dati vengono salvaguardati anche attraverso il loro salvataggio con le modalità descritte al punto 9.

12 Trattamenti senza l'ausilio di strumenti elettronici
(modalità applicative delle regole di cui ai punti 27, 28, 29 dell'All. B)

12.1 Istruzioni agli incaricati del trattamento

Agli incaricati del trattamento sono impartite istruzioni scritte finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo sviluppo dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dai medesimi incaricati fino alla restituzione in modo che a essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

13 Diritti dell'interessato

13.1 Diritto di accesso ai dati personali

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.

13.2 Esercizio dei diritti

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.

13.3 Modalità d'esercizio

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.

13.4 Riscontro dell'interessato

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.

14 Amministratore di Sistema

Il Garante con il provvedimento del 27/11/2008 e modificato con provvedimento del 25/06/2009 prescrive l'adozione di misure specifiche relativamente alle attribuzioni di funzioni di amministratore di sistema.

Il provvedimento prescrive l'adozione di tali misure ai "*titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice),* ***salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte di recente per legge*** *(art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008)"*.

Si riporta di seguito la definizione di "**trattamenti effettuati per finalità amministrativo-contabili**" contenuta nell art.34 al comma 1-ter: "*Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro*."

Ciò premesso, dato che la tipologia di trattamento effettuato dall'azienda (vedere anche cap.3) si configura come effettuato esclusivamente per finalità amministrativo-contabili, le misure specifiche previste dal Garante relativamente alle attribuzioni di funzioni di amministratore di sistema non sono applicabili.

15 Videosorveglianza (provv.to del Garante del 08/04/2010)

Dopo un primo provvedimento del 29.11.2000 ad integrazione ed aggiornamento dello stesso, il Garante emanava il "Provvedimento generale sulla videosorveglianza – 29 Aprile 2004". E' stato adesso adottato un nuovo "Provvedimento in materia di videosorveglianza – 8 Aprile 2010" (pubblicato sulla Gazzetta Ufficiale n.99 del 29.4.2010) che sostituisce i precedenti ed emana nuove regole.

I principi generali cui deve attenersi ogni tipo di trattamento dei dati sono:

- Principio di **necessità**, che esclude ogni uso eccessivo e superfluo;
- Principio di **proporzionalità**, per il quale il trattamento deve essere proporzionato agli scopi prefissi e legittimamente perseguibili;
- Principio di **finalità**, che richiede scopi determinati, espliciti e legittimi;
- Principio di **liceità**, che nel Codice pone i presupposti del trattamento lecito dei dati.

Si riportano di seguito i principali adempimenti:

Predisporre l'informativa, posta a tutela del diritto del cittadino di sapere che sta entrando o si trova in una zona videosorvegliata. Il Garante offre un modello di informativa "minima" per le aree esterne, ovvero un cartello posizionato prima del raggio d'azione con caratteri ben visibili che si possa vedere anche di notte qualora la videosorveglianza rimanga attiva. Tale modello, se utilizzato nelle aree interne, deve essere integrato con gli elementi dell'art. 13 del Codice Privacy.

Adottare misure di sicurezza a protezione dei dati registrati tramite impianti di videosorveglianza, ad esempio l'utilizzo di sistemi automatici di cancellazione dei dati allo scadere del tempo massimo di conservazione stabilito, creazione di password d'accesso etc.

I dati raccolti possono essere conservati per il solo tempo strettamente necessario per perseguire il fine,

massimo 24 ore. Tempi più lunghi (massimo 7 giorni) devono essere giustificati da elementi validi e necessità particolari (ad esempio per uffici o esercizi quando la chiusura avviene i giorni festivi).

Devono essere indicate per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti, e nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni.

La videosorveglianza è consentita, senza necessità di alcun consenso, qualora essa sia effettuata nell'intento di perseguire fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, atti di vandalismo, prevenzione di incendi, sicurezza del lavoro.

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, "*dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti*".

Il mancato adempimento può determinare: un trattamento illecito e quindi la inutilizzabilità dei dati; un trattamento non corretto, quindi provvedimenti di blocco o divieto da parte del Garante; possibili decisioni dell'autorità giudiziaria civile e penale. La sanzione prevista varia da 5.000 a 30.000 euro ai sensi dell'art. 161 del Codice Privacy.

16 Allegati

- Allegato **INC** - Elenco degli incaricati al trattamento
- Allegato **IDT** - Lettere incarico per gli incaricati del trattamento
- Allegato **EST** - Lettere d'indicazione del responsabile esterno per il trattamento dati
- Allegato **VDS** - Lettera incarico per la videosorveglianza
- Allegato **REST** - Nomina Responsabile esterno per la gestione dei sistemi informatici
- Allegato **DISC** - Disciplinare email internet