

ASSOCIAZIONE NAZIONALE «CNOS/Scuola»

Centro Nazionale Opere Salesiane - Scuola

Via Marsala, 42

00185 ROMA

Sede nazionale

E-mail cnos-scuola@salesiani.it

Tel. **06/44.40.354**

Prot. 65/04

INFORMAZIONI CNOS/Scuola

A cura della Segreteria CNOS/Scuola

n. 8/2004 - 15 marzo 2004

INDICE

[89/04 Codice sulla privacy e adempimenti delle istituzioni scolastiche](#)

[90/04 La presentazione del Codice sulla privacy \(DLvo n. 196/2003\)](#)

[91/04 La struttura del Codice sulla privacy](#)

[92/04 Il Documento Programmatico sulla Sicurezza \(DPS\)](#)

[93/04 L'indice del DPS](#)

[94/04 Allegato 1: Definizioni \(articolo 4, DLvo n. 196/2004\)](#)

[95/04 Allegato 2: Istruzione \(articoli 95-96, DLvo n. 196/2004\)](#)

[96/04 Allegato 3: Allega B del Codice sulla privacy](#)

TESTO

[89/04 Codice sulla privacy e adempimenti delle istituzioni scolastiche](#)

Il *Trattamento dati nelle istituzioni scolastiche* rappresenta un'*Istruzione* che viene inserita nel Manuale di qualità delle Scuole Salesiane.

Tuttavia si deve subito comprendere che gli adempimenti ivi prescritti non sono dovuti alle Norme ISO 9000:2000, ma al DLvo n. 196/2003 e, di conseguenza, costituiscono obblighi sanzionati per tutte le istituzioni scolastiche, indipendentemente dalla certificazione di qualità.

Una direzione di marcia è rappresentata dalla informatizzazione dell'intera gestione dell'attività scolastica, che rende possibile una semplificazione degli adempimenti (registro on line scuola-famiglia, Manuale di qualità on line, informatizzazione della segreteria e dell'amministrazione, informatizzazione della gestione dell'intera attività scolastica inserita nel POF).

Questa *Istruzione*, resa possibile dall'apporto professionale della dott.ssa Daniela Votano, si compone di tre parti:

- La presentazione del Codice sulla privacy (DLvo n. 196/2003)
- La struttura del Codice sulla privacy
- Il Documento Programmatico sulla Sicurezza (DPS)
- L'indice del DPS
- Allegato 1: Definizioni (articolo 4, DLvo n. 196/2004)
- Allegato 2: Istruzione (articoli 95-96, DLvo n. 196/2004)

Ricordiamo che il testo del DLvo n. 196/2004 è inserito anche nella mediateca del sito www.didalabor.com

90/04 La presentazione del Codice sulla privacy (DLvo n. 196/2003)

Con il 1 gennaio 2004 è entrato in vigore il Decreto legislativo 30 giugno 2003, n. 196 (*Gazzetta Ufficiale* 29 luglio 2003, n. 174 - Supplemento ordinario n. 123/L) [Codice in materia di protezione dei dati personali](#) meglio noto come "Codice sulla privacy" (denominato di seguito "Codice").

Si tratta di un provvedimento assai corposo (ben 186 articoli) al quale si aggiungono tre allegati:

Il nuovo Codice incide in maniera significativa sull'impianto normativo preesistente, quello, per intenderci, tracciato dalla legge n. 675/1996 e dal DPR n. 318/1999 ora non più validi.

Per un confronto puntuale tra la normativa precedente e quella del Codice si può consultare utilmente il sito www.garanteprivacy.it - In evidenza: il nuovo codice della privacy – decreto legislativo n. 196 del 30 giugno 2003 - [Tavola di corrispondenza dei riferimenti previgenti al codice in materia di protezione dei dati personali.](#)

Tutta la legislazione che riguarda la materia complessa del trattamento e della protezione dei dati personali confluisce in un'unica raccolta.

Partendo dal concetto che ogni soggetto ha diritto alla protezione dei dati personali che lo riguardano, il Codice si ispira ai principi di semplificazione, armonizzazione ed efficacia, snellendo parecchio le modalità di adeguamento e di adempimento degli obblighi da parte dei titolari del trattamento (articoli 1.3).

Un esempio per tutti: viene «ribaltato» il principio dell'obbligo della notificazione al Garante. Inizialmente quest'obbligo vigeva *erga omnes*, salvo poche e rare eccezioni; ora, intuita l'eccessività e l'inutilità dell'adempimento, la notificazione non va fatta, eccetto i casi espressamente contemplati dal Codice.

91/04 La struttura del Codice sulla privacy

1. Principi generali

La prima parte contiene le disposizioni generali (articoli da 1 a 45), riguardanti le regole sostanziali della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, nonché le regole

specifiche che si devono osservare per i trattamenti effettuati da soggetti pubblici e quelle che trovano applicazione per i soggetti privati ed enti pubblici economici.

Ambito di applicazione del Codice (articolo 5)

Sono tenuti ad adeguarsi tutti coloro che trattano dati personali, indipendentemente dalle dimensioni dell'attività (piccola, media o grande impresa, attività artigianale, impresa familiare, liberi professionisti, ecc.) e dal numero di lavoratori.

Gli adempimenti sono diversi a seconda delle dimensioni della struttura, dell'organigramma adottato, e della tipologia di trattamento dei dati.

Il dettato normativo deve essere adeguato alle reali esigenze di ogni attività. Non avrebbe senso, infatti, omologare l'adeguamento riportandosi pedissequamente a schemi che non soddisfano gli adempimenti.

Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano, in ogni caso, le disposizioni in tema di responsabilità e sicurezza dei dati.

Ambito di applicazione della legge italiana (articolo 5)

La legge n. 675/1996 congiungeva l'applicabilità della legge italiana a tutti quei casi in cui fosse svolta nel territorio italiano una frazione del trattamento di dati. Il Codice, all'articolo 5, ha ribadito, quale criterio principale di collegamento della fattispecie alla legge applicabile, lo stabilimento nel territorio dello Stato, o in luogo soggetto alla sua sovranità, del soggetto che effettua il trattamento. Qualora il soggetto che effettui il trattamento sia stabilito in altro Paese dell'UE, si applicherà la legge del Paese di stabilimento. Nel caso in cui il soggetto sia stabilito in Paesi non UE, il Codice sarà applicabile nel caso in cui vengano impiegati per il trattamento strumenti situati nel territorio dello Stato (italiano), anche diversi da quelli elettronici, escluso il mero transito nell'UE.

La notificazione (articolo 37)

Come prescritto, il titolare deve notificare al Garante solamente in alcuni casi il trattamento di dati personali, cioè quando si tratta di «dati sensibili» e specificatamente se riguarda :

- a) «dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti».

La notificazione, inoltre, dovrà essere effettuata sia in particolari casi di trattamento di dati sensibili (specie se sanitari) con determinate modalità d'uso, ma anche per trattamenti particolarmente a rischio,

effettuati con strumenti elettronici, nel campo della profilazione dei consumatori, oppure in relazione a procedure di selezione del personale e ricerche di marketing, nonché in ipotesi di utilizzo di informazioni commerciali e relative alla solvibilità.

L'informativa (articolo 13)

Una delle novità introdotte dal Codice è lo snellimento della raccolta dei dati tra gli interessati. L'informativa è la dichiarazione che il titolare e/o il responsabile del trattamento fa all'interessato, in forma scritta od orale, intorno alle caratteristiche sull'utilizzo dei dati che lo riguardano. Il contenuto dell'informativa è tassativamente prescritto dal Codice. La *ratio* consiste nella necessità di assicurare all'interessato l'esercizio del controllo sui suoi dati. Quest'ultimo, infatti, può esercitare il diritto all'autodeterminazione informativa e, attraverso l'articolo 7, far valere il diritto di accesso e di opposizione al trattamento avendo sempre diritto ad ottenere la cancellazione gratuita dei dati. Il rilascio dell'informativa, esercitato nelle forme previste dal codice, costituisce la condizione della validità del consenso prestato e, nel contempo, l'esercizio dei diritti di cui all'articolo 7.

2. Settori specifici quali la Sanità, Giustizia e Pubblica Amministrazione (PA)

La seconda parte è dedicata a specifici settori (articoli da 46 a 140): la sezione, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori

Settore sanitario

In ambito sanitario si semplifica l'informativa da rilasciare ai pazienti e si consente di manifestare il consenso al trattamento dei dati con un'unica dichiarazione resa al medico di famiglia o all'organismo sanitario (il consenso vale anche per la pluralità di trattamenti a fini di salute erogati da distinti reparti e unità dello stesso organismo, nonché da più strutture ospedaliere e territoriali).

Vengono inoltre codificate misure per il rispetto dei diritti del paziente: distanze di cortesia, niente appelli nominativi dei pazienti in sala di attesa, certezze e cautele nelle informazioni telefoniche e nelle informazioni sui malati ricoverati, estensione delle esigenze di riservatezza anche agli operatori sanitari non tenuti al segreto professionale.

Viene introdotta la possibilità di non rendere immediatamente identificabili in farmacia gli intestatari di ricette.

Per i dati genetici viene previsto il rilascio di un'apposita autorizzazione da parte del Garante, sentito il Ministro della salute.

Trattamento dei dati in ambito giudiziario

Superata la legge n. 675/1996 in materia giudiziaria che conteneva solo dichiarazioni d'intenti, adesso le parti sono garantite in modo più puntuale ed esaustivo.

Il Codice, all'articolo 52, prevede infatti che l'interessato possa chiedere, nel processo, di apporre sulla sentenza un'annotazione con la quale si avvisa che, nel caso di pubblicazione del verdetto su riviste giuridiche o su supporti elettronici o in caso di diffusione mediante reti telematiche, devono essere omessi i suoi dati. Quando, invece, il processo verte su ambiti di violenza sessuale, su minori o su rapporti di famiglia o di stato delle persone, allora la sentenza deve sempre essere diffusa con i nomi oscurati

Pubblica Amministrazione

Il Codice sottolinea e ribadisce che l'utilizzo dei dati sensibili archiviati e custoditi dagli uffici pubblici avvenga sempre e soltanto a determinate condizioni:

- perseguimento della rilevante finalità pubblica;
- indicazione degli utilizzi possibili.

Ne derivano importanti conseguenze sul piano operativo: la PA deve dotarsi di regolamenti ad hoc, con il parere conforme del Garante, per il trattamento dei dati sensibili.

3. La scuola (articoli 95-96)

Le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 13. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza.

Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

4. Tutela e sanzioni

La terza parte affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante

Le disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio (articoli da 141 a 172), alle quali si aggiungono le norme di modifica, finali e di carattere transitorio (articoli da 173 a 186).

È stata rafforzata la tutela contro le comunicazioni indesiderate (spamming), ribadendo il principio all'articolo 130 del codice, dell'opt-in (il consenso degli interessati), per cui è consentito l'invio di comunicazioni mediante sistemi automatizzati (posta elettronica, fax, dispositivi automatici di chiamata) solo con il preventivo consenso dell'utente interessato: tale tutela è stata estesa anche all'invio di messaggi pubblicitari tramite Sms e Mms. Cade in maniera definitiva ed assoluta l'ipotesi dell'opt-out: continuare ad inviare materiale fino a quando l'interessato dica basta.

▪ **Principali sanzioni**

- ❑ Multe da 3.000 a 0.0000 euro (elevabile al triplo).
- ❑ Reclusione fino a 3 anni.
- ❑ Possibilità di estinguere il reato penale, adeguandosi alla normativa e pagando una sanzione pecuniaria.
- ❑ Risarcimento del danno cagionato ex art. 2050

▪ **Trattamento illecito di dati**

Reclusione da 6 a 18 mesi o, se il fatto consiste nella comunicazione o diffusione, fino a 36 mesi

▪ **Falsità nelle dichiarazioni al Garante**

Reclusione da 6 mesi a 3 anni

▪ **Misure di sicurezza**

Arresto sino a 2 anni o ammenda da 10.000 a 50.000 Euro

▪ **Inosservanza di provvedimenti del Garante**

Reclusione da 3 mesi a 2 anni

▪ **Violazioni amministrative**

- ❑ Omessa/inidonea informativa
- ❑ Sanzione da 3.000,00 a 18.000,00 Euro
- ❑ Sanzione da 5.000,00 a 30.000,00 Euro con la possibilità di aumentare fino al triplo, se in violazione di dati sensibili o giudiziari

5. Allegati

Vi sono infine degli Allegati, parte integrante del Codice, che andranno adeguatamente implementati dai Codici di deontologia.

Allegato A

- A1: relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica;
- A2: per il trattamento dei dati personali per scopi storici;
- A3: per il trattamento dei dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema Statistico Nazionale

Allegato B

L'allegato B è un disciplinare tecnico in materia delle misure minime di sicurezza da adottare. Direttamente richiamato il DPR n. 318/1999 con il suo DPS (Documento Programmatico sulla Sicurezza).

Entro il 31 marzo di ogni anno, il Titolare o il Responsabile (ove sia stato designato) di un trattamento di dati sensibili e/o giudiziari, redige un idoneo Documento Programmatico sulla Sicurezza DPS), che contiene una sorta di «stato dell'arte» a riguardo dell'elenco del trattamento dei dati personali, della distribuzione di compiti e responsabilità, dell'analisi dei rischi incombenti sui dati e delle misure di sicurezza adottate per garantire l'integrità dei dati, nonché la protezione dei locali e delle aree.

L'articolo 26, sempre dell'allegato B, nelle ulteriori misure in caso di trattamento di dati sensibili o giudiziari, dispone che il titolare deve riferire, nella relazione accompagnatoria al bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del Documento programmatico sulla sicurezza

Allegato C

Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia

6. Entrata in vigore e calendario delle scadenze

Le disposizioni del nuovo codice sono entrate in vigore dal 1 gennaio 2004.

Per l'adeguamento alle nuove norme è possibile chiedere una proroga, *ex articolo* 180 del testo unico sulla privacy, al 1° gennaio 2005, se al 31 dicembre 2003 non si è in grado di adeguare il proprio sistema informatico o si evidenziano altre difficoltà. In questi casi, con un documento avente data certa, si chiede la proroga.

Per i trattamenti di dati personali iniziati prima del 1 gennaio 2004, in sede di prima applicazione del presente codice:

- a) l'identificazione - con atto di natura regolamentare dei tipi di dati e di operazioni ai sensi degli articoli 20, commi 2 e 3, e 21, comma 2 - è effettuata, ove mancante, **entro il 30 settembre 2004;**
- b) la determinazione da rendere nota agli interessati ai sensi dell'articolo 26, commi 3, lettera a), e 4, lettera a), è adottata, ove mancante, **entro il 30 giugno 2004;**
- c) le notificazioni previste dall'articolo 37 sono effettuate **entro il 30 aprile 2004;**
- d) le comunicazioni previste dall'articolo 39 sono effettuate **entro il 30 giugno 2004;**

- e) le modalità semplificate per l'informativa e la manifestazione del consenso, ove necessario, possono essere utilizzate dal medico di medicina generale, dal pediatra di libera scelta e dagli organismi sanitari anche in occasione del primo ulteriore contatto con l'interessato, al più tardi **entro il 30 settembre 2004;**
- f) l'utilizzazione dei modelli di cui all'articolo 87, comma 2, è obbligatoria **a decorrere dal 1 gennaio 2005.**

L'individuazione dei trattamenti e dei titolari è effettuata in sede di prima applicazione del presente codice entro il 30 giugno 2004.

Il Codice prevede due principali scadenze a carico delle aziende [istituzioni scolastiche] in tema di sicurezza e di misure di sicurezza.

- a) Entro il 30 giugno 2004 **deve essere adottato il sistema di misure di sicurezza minime obbligatorie previste dal Codice**, salvi i casi di impossibilità tecnica dovuta al sistema informatico. In questo caso va redatto un apposito documento, di data certa da conservare presso l'azienda [istituzione scolastica], dove vanno evidenziati i problemi di natura tecnica. Ciò consente lo slittamento del termine al 1 gennaio 2005.

Le misure minime di sicurezza vengono dettagliatamente descritte nel disciplinare tecnico contenuto nell'allegato B. La loro inosservanza costituisce reato punito con l'arresto sino a due anni, ovvero con una ammenda da 10.000 a 50.000 euro.

- b) **Entro il 31 marzo 2004** (prima scadenza), e successivamente entro il 31 marzo di ogni anno, qualora il trattamento contenga dati sensibili o giudiziari e sia effettuato con strumenti elettronici, il titolare deve redigere il **Documento Programmatico sulla Sicurezza.**

7. Riflessioni conclusive

Il Codice sulla tutela della privacy, al pari di ogni altra legge, è inderogabile e cogente, comminando in alcuni casi d'infrazione anche sanzioni rilevanti.

Nonostante già esistano ragioni di ordine normativo/coercitivo per adeguarsi, si vuole qui suggerire un'ulteriore motivazione, che possa fungere da spunto riflessivo: non sarebbe una contraddizione in termini soprattutto economici adeguare la propria istituzione scolastica, dal punto di vista della sicurezza (si pensi alla normativa sulla sicurezza dei lavoratori e dei luoghi di lavoro o alla messa a norma degli impianti elettrici) e poi tenere il fianco scoperto per tutto ciò che attiene ai dati personali? inoltre, non sarebbe potenzialmente pericoloso non formare i propri dipendenti/collaboratori sulla privacy? (si pensi soprattutto a tutte le attività caratterizzate da un elevato front-office e/o contatto con il pubblico)

Se ne deduce che dal prossimo futuro sarà importante orientare le scelte di adeguamento e formazione del personale ad un principio già evidenziato dal Garante nello scorso anno: concepire l'adeguamento alla tutela della privacy come investimento e maggiore tutela dei propri clienti e non meramente come costo a carico dell'azienda.

[92/04 Il Documento Programmatico sulla Sicurezza \(DPS\)](#)

I contenuti contenuti

Il documento programmatico sulla sicurezza definisce le politiche di sicurezza adottate dal titolare in materia di trattamento dei dati personali. Nel documento programmatico si esplicitano le misure di sicurezza adottate e quelle che si intende adottare per garantire un adeguato livello di protezione per i dati personali al cui trattamento si procede.

Il documento programmatico, pertanto, presenta in primo luogo **un'analisi della situazione attuale dell'istituzione scolastica e dei trattamenti in corso presso il titolare**. Punto di partenza del documento programmatico è la descrizione del sistema informatico presente nell'impresa, sia nelle sue componenti hardware che in quelle software, e la definizione di un elenco dei trattamenti di dati personali riferibili al titolare.

La redazione del **documento programmatico**, inoltre, consiste in un processo dinamico: oltre ad una descrizione delle misure in essere, infatti, il titolare **esplicita le misure che intende adottare nel quadro di un piano di riferimento per garantire la sicurezza dei dati**.

Il documento programmatico sulla sicurezza deve contenere idonee informazioni in merito ai seguenti aspetti:

1. L'elenco dei trattamenti dei dati personali

Si fa riferimento a tutti i trattamenti di dati personali (sensibili e non) che hanno luogo presso il titolare. Si ricorda che la definizione di trattamento è ampia (cfr. articolo 4, lettera a) del Codice, secondo la quale è trattamento dei dati ogni operazione (...) «concernente 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 dei dati»).

Si procederà dunque ad un censimento dei trattamenti individuando, per ogni categoria, le modalità specifiche di trattamento e descrivendo le tipologie di dati considerati.

Il livello di cautele da adottare per predisporre misure di sicurezza idonee varia a seconda della tipologia di dati che vengono trattati. Tali misure, pertanto, dovranno assumere un carattere crescente a seconda che si tratti di dati personali comuni, giudiziari, sensibili oppure sulla salute o sulla vita sessuale o riguardanti il menoma (i dati appartenenti a queste ultime tre categorie ricevono una specifica disciplina nel disciplinare tecnico). Nell'effettuare il censimento dei trattamenti interni alla struttura, pertanto, sarà opportuno specificare la natura dei dati al cui trattamento si procede

2. La distribuzione di compiti e responsabilità all'interno della struttura

Sarà necessario **esplicitare gli elementi portanti della struttura organizzativa aziendale in materia di privacy, menzionando i soggetti che hanno specifiche responsabilità nel trattamento dei dati personali** (titolare, responsabili, incaricati suddivisi per classi omogenee, altri soggetti che svolgono un ruolo peculiare).

Si ricorda che il Codice contiene disposizioni specifiche in materia di organizzazione interna e disciplina le figure del responsabile (articolo 29) e dell'incaricato al trattamento dei dati personali (art. 30).

La nomina di uno o più responsabili, in particolare, consente al titolare di razionalizzare la struttura interna delegando parzialmente compiti e responsabilità. Sarà necessario, inoltre, definire le categorie di incaricati suddividendoli per classi omogenee a seconda delle tipologie di trattamento dei dati a cui accedono. In questa sezione del documento, pertanto, si ripercorreranno le scelte organizzative già effettuate al momento della definizione delle classi di incaricati e dei diversi profili di autorizzazione.

Devono inoltre essere incluse le dichiarazioni di nomina dei responsabili (in cui si esplicitano - per iscritto - le istruzioni relative al trattamento ed i criteri da seguire) e le designazioni/istruzioni impartite - per iscritto - agli incaricati ed agli altri soggetti che, a vario titolo, svolgono una funzione peculiare nella struttura. Basti pensare al ruolo del custode delle credenziali per l'accesso ovvero, qualora uno o più trattamenti (o parti di un trattamento) si svolgano al di fuori della struttura, ad altri soggetti esterni (chi procede all'assistenza nella predisposizione del software o nell'elaborazione delle pagine).

Si dovranno infine specificare le responsabilità collegate al ruolo svolto da ciascuna figura all'interno della struttura aziendale.

3. L'analisi dei rischi incombenti sui dati

Nel documento programmatico vanno esplicitate le misure minime da adottare a garanzia dell'integrità e della disponibilità dei dati. La fase di analisi dei rischi svolge un ruolo centrale nella definizione del documento programmatico e delle linee guida che si intendono adottare per predisporre misure tali da garantire la sicurezza dei dati trattati.

I possibili rischi che gravano sui dati (direttamente o, indirettamente se riferiti alle strutture mediante le quali si procede al trattamento) sono numerosi e difficilmente catalogabili. Essi possono essere ricondotti alle seguenti categorie:

- danneggiamento e/o sottrazione delle strutture di hardware;
- danneggiamento (doloso, colposo o accidentale) del server, del software e dei dati contenuti al loro interno;
- conseguenze negative di ogni tipo derivanti da accessi non autorizzati (di soggetti con profilo diverso di autorizzazione o di altri soggetti esterni alla struttura);
- distruzione, alterazione, diffusione e/o comunicazione non autorizzata dei dati, anche di quelli meramente personali.

4. Le misure di sicurezza adottate e da adottare

Lo sviluppo di questa sezione rappresenta una diretta conseguenza dell'attività di individuazione dei rischi svolta nella parte precedente. Si dovranno identificare misure tali da garantire l'integrità dei dati, la loro disponibilità, nonché la protezione delle strutture in cui i dati vengono custoditi e mediante le quali si accede agli stessi.

Dopo aver definito le misure necessarie, pertanto, si espliciteranno le modalità nelle quali le misure minime di sicurezza vengono realizzate nella realtà organizzativa dell'impresa.

In particolare, per quanto riguarda le misure minime per il trattamento effettuato con strumenti informatici, le disposizioni del Codice impongono di individuare:

- le credenziali di autenticazione (scegliendo tra le tipologie previste nel disciplinare tecnico) e le modalità di gestione delle stesse;
- un sistema di autorizzazione, definendo i profili per classi e mantenendoli aggiornati;
- le regole relative all'impiego ed all'aggiornamento dei programmi antivirus, dei programmi di antintrusione e degli aggiornamenti/upgrade dei programmi.

Quanto ai criteri per la protezione delle aree e dei locali essi sono assai vari ed andranno individuati a seconda della strumentazione posseduta e delle circostanze presenti nel caso concreto. Ci si dovrà occupare, pertanto, dei sistemi per la **protezione del server** (protezione dei locali, previsione di procedure di accesso, sistemi antincendio, servizi di vigilanza etc.), delle **strutture di rete** (sistemi di firewall, procedure specifiche per chi accede alle infrastrutture, etc) e **dei singoli elaboratori** situati negli uffici e negli altri locali dell'azienda (allarmi antifurto, sistemi di vigilanza, gruppi di continuità etc).

Si ricorda, inoltre, che le misure di sicurezza vanno adottate non solo in riferimento agli elaboratori presenti nell'azienda ma anche in riferimento ad altri strumenti elettronici (computer palmari, notebook etc.) detenuti a vario titolo da responsabili e/o incaricati sui quali transitano dati personali.

5. Criteri e modalità per il ripristino dei dati distrutti o danneggiati

In questa sezione vanno definiti i criteri e le procedure per assicurare l'integrità e la disponibilità dei dati in caso di loro distruzione e/o danneggiamento. Il disciplinare tecnico, infatti, dispone l'adozione di procedure in grado di garantire il ripristino dei dati nel caso di danni a questi ultimi o alle strutture mediante le quali si procede al trattamento. Andranno pertanto descritte le procedure per l'esecuzione del backup dei dati e la sua conservazione. **Si ricorda che le procedure per il ripristino dei dati**

devono essere compatibili con i diritti dell'interessato e, in ogni caso, contenute nel limite di sette giorni.

6. La previsione di interventi formativi per gli incaricati del trattamento

Gli adempimenti in termini di formazione nei confronti degli incaricati vengono ora definiti in maniera specifica. Nella sezione del documento programmatico, pertanto, si dovrà definire il numero, le tipologie ed i contenuti degli incontri formativi a cui si intende procedere.

Sarà opportuno conservare tutta la documentazione di cui ci si è avvalsi nell'attività di formazione e prevedere sistemi per registrare la partecipazione, così da poter provare l'avvenuta formazione degli incaricati.

Il disciplinare tecnico dispone che la formazione debba avere carattere di periodicità ed essere fornita in determinate occasioni (attribuzione dell'incarico; cambiamento del profilo di autorizzazione; introduzione di nuovi strumenti, rilevanti rispetto al trattamento di dati personali)

7. Criteri per garantire l'adozione delle misure minime nel caso di trattamenti affidati all'esterno della struttura

Il documento programmatico sulla sicurezza impone di descrivere i criteri da adottare per garantire il rispetto delle misure minime nel caso in cui alcuni trattamenti (o parti di esso) siano effettuati all'esterno della struttura. Il caso è tutt'altro che raro, basti pensare, ad esempio, ai casi di si avvale di un supporto esterno nella gestione delle paghe.

Una modalità per garantire l'adozione di misure minime da parte dei soggetti esterni è di predisporre apposite clausole contrattuali mediante le quali concordare determinati comportamenti in materia di sicurezza nel trattamento dei dati.

[93/04 L'indice del DPS](#)

Nel dettaglio, si compila un documento le cui linee guida sono le seguenti:

1. titolari del trattamento
2. ruoli dei titolari
3. ruoli dei responsabili di sicurezza dei dati personali
4. ruoli dei responsabili di gestione e manutenzione di strumenti elettronici
5. ruoli degli incaricati della custodia di copia delle credenziali
6. ruoli degli incaricati di copia della sicurezza della banche dati
7. ruoli dei responsabili del trattamento dei dati personali
8. ruoli degli incaricati (soggetti che trattano dati sia cartacei che informatizzati):
9. sedi/ uffici
10. responsabili di accesso ai locali
11. software utilizzato
12. sistemi elaborazione (pc)
13. istruzioni di back-up
14. banche dati
15. permessi di accesso
16. attacchi/virus
17. piano di formazione personale
18. rischi software/ rischi hardware
19. lettere di incarico a tutte le figure (dal punto 8 al punto 13), controfirmate per accettazione

20. lettere di incarico a tutti i responsabili di trattamenti esterni (ad esempio consulenti del lavoro, consulenti fiscali, esperti sistemi informatici, ecc)

1. Misure minime di sicurezza (articolo 33-36)

Le misure minime previste dal Codice sono in concreto individuate dal disciplinare tecnico allegato B, e sono volte ad assicurare un livello (appunto) minimo di protezione dei dati personali (articolo 33), un livello al di sotto del quale non si può scendere in quanto, come si è detto, il mancato rispetto di dette misure costituisce reato.

La misure minime di sicurezza riguardano:

- i Trattamenti con strumenti elettronici (articolo 34)
- e Trattamenti senza l'ausilio di strumenti elettronici (articolo 35)

L'articolo 36 ricorda che «il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del 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».

Trattamenti con strumenti elettronici (articolo 34)

Tra [] il nostro commento.

«Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) autenticazione informatica;
 - [Assegnazione di ID (Identification Card) e password ad ogni incaricato del trattamento,
 - Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata, conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave]
- b) adozione di procedure di gestione delle credenziali di autenticazione [procedure di assegnazione e gestione credenziali di autenticazione];
- c) utilizzazione di un sistema di autorizzazione [autorizzazione per ogni incaricato a trattare dati, attraverso nomina scritta controfirmata per accettazione];
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici [controllo periodico dell'uso della password e revoca a chi non ne fa uso per 6 mesi.(o, in caso di dati sensibili, 3 mesi)];
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di I dati, ad accessi non consentiti e a determinati programmi informatici [inserimento di password di sistema, installazione ed aggiornamento di antivirus];
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi [copie di back-up, archiviazione e custodia delle copie di back-up];
- g) tenuta di un aggiornato documento programmatico sulla sicurezza [redazione e/o aggiornamento e corretta custodia del documento programmatico sulla sicurezza];
- h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari [Trattamento di dati sensibili attraverso un sistema di codificazione degli stessi – es. al nominativo si sostituisce un codice]».

Con particolare puntigliosità vengono specificate le caratteristiche che deve avere una password per essere considerata realmente tale. A norma del Disciplinare Tecnico, infatti, la parola-chiave dovrà essere 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, inoltre, non dovrà contenere riferimenti agevolmente riconducibili all'interessato (ad esempio, nome della moglie, marca dell'autovettura, squadra di calcio della quale si è tifosi, ecc.) e dovrà essere per legge modificata almeno ogni sei mesi (Allegato B, 5).

Un'ulteriore disposizione riguarda l'obbligatorietà di effettuare, almeno ogni settimana, copie di backup dei dati contenuti nei propri sistemi informatici (Allegato B, 18).

Trattamenti senza l'ausilio di strumenti elettronici (articolo 35)

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

2. Misure idonee

Il Codice impone al titolare del trattamento dei dati personali di predisporre tutte le misure di sicurezza idonee a ridurre al minimo “i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta” (articolo 31 *Obblighi di sicurezza*).

Si tratta in sostanza di adottare tutte quelle misure che permettono la migliore custodia e il massimo controllo dei dati oggetto di trattamento sulla base delle conoscenze acquisite in base al progresso tecnico.

Se l'adeguamento alle “misure minime” implica l'assenza di responsabilità penali, tale adeguamento non è tuttavia sufficiente per affrancarsi dalla responsabilità civile. Qualora infatti gli accorgimenti presi non soddisfino le misure dichiarate “idonee” può trovare applicazione l'articolo 2050 del *codice civile*. In base a tale norma è tenuto al risarcimento di ogni danno eventualmente cagionato a terzi chiunque non riesca a dar prova di aver adottato “tutte le misure” idonee ad evitare il danno stesso.

3. I minori (articolo 50)

L'articolo 50 *Notizie e immagini relative ai minori* dispone: «Il divieto di cui all'articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448, di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale».

4. La videosorveglianza (articolo 134)

Riguarda le istituzioni scolastiche solamente se sono dotate di sistemi di videosorveglianza a circuito chiuso.

Una nuova disciplina legale è dedicata dal Codice alla “videosorveglianza”, la quale come noto consiste nell'installazione di sistemi, reti ed apparecchiature che permettono la ripresa e l'eventuale registrazione di immagini in particolare ai fini di sicurezza.

Al riguardo, il Codice deferisce al Garante il compito di emanare un codice di deontologia volto a disciplinare il fenomeno, prevedendo specifiche modalità di trattamento e forme semplificate di disciplina.

Allo stato, le indicazioni più interessanti in materia sono contenute nel “provvedimento generale del 29 novembre 2000” (facilmente reperibile al sito www.garanteprivacy.it), che prevede una sorta di “decalogo di regole” per non violare la privacy nell’effettuare la videosorveglianza.

Viene trascritto il testo dell’articolo 134 *Codice di deontologia e di buona condotta*: «Il Garante promuove, ai sensi dell’articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all’interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall’articolo 11».

[94/04 Allegato 1: Definizioni \(articolo 4, DLvo n. 196/2004\)](#)

Articolo 4. Definizioni

1. Ai fini del presente codice si intende per:

- a) "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;
- b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
- d) "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;
- e) "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;
- f) "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;
- g) "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;

- h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- l) "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;
- m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

- a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- b) "chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- c) "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- d) "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- e) "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare

radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

- f) "abbonato", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
- g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- h) "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- i) "dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
- l) "servizio a valore aggiunto", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:

- a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- e) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- f) "profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- g) "sistema di autorizzazione", 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.

4. Ai fini del presente codice si intende per:

- a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- b) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- c) "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

[95/04 Allegato 2: Istruzione \(articoli 95-96, DLvo n. 196/2004\)](#)

TITOLO VI - ISTRUZIONE

CAPO I - PROFILI GENERALI

Articolo 95. Dati sensibili e giudiziari

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario, con particolare riferimento a quelle svolte anche in forma integrata.

Articolo 96. Trattamento di dati relativi a studenti

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 13. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

(Articoli. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

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

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. 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.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso

della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. 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.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza

contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di 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 di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei 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;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. 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.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati

idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi

all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

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

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

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

29. 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.