IL DECRETO LEGGE 196/2003

Scopo del presente documento

Compiere un'analisi sommaria del Decreto Legislativo 196/2003 per quanto attiene alle disposizioni relative alla protezione dei sistemi informativi e dei dati in essi contenuti, al fine di consentire alle Aziende ed agli Enti interessati di valutare se:

- l'ambito di applicazione del Decreto Legislativo coinvolga il proprio sistema informativo
- le nuove disposizioni richiedano un intervento sul proprio sistema informativo.

Esula dagli scopi del documento dare indicazioni riguardo ad interventi specifici da operare per l'adeguamento del sistema informativo ai disposti della Normativa; tali indicazioni, diversificate in funzione del tipo di dati custoditi ed all'ambito operativo dell'Ente o dell'Azienda - giudiziario, sanitario, Forza Pubblica, Pubblica Amministrazione, bancario/assicurativo e così via -, possono infatti essere elaborate solo a seguito di un'analisi da condursi caso per caso.

Non viene inoltre affrontata alcuna questione riguardante la natura dei dati.

Struttura del presente documento

- Trascrizione dei principali Articoli di Legge oggetto della successiva analisi, utili al raggiungimento dello scopo del presente documento
- Identificazione dei dati oggetto del Decreto Legislativo, distinti tra "dati personali" e "dati sensibili" – entrambi soggetti ai disposti del Decreto Legislativo -
- Identificazione dei destinatari degli obblighi previsti dal Decreto Legislativo, ovvero di quelle Società ed Enti che sono tenuti a conformarsi ai principi ed ai contenuti del Decreto Legislativo
- Principali adempimenti a carico dei titolari di sistemi informativi aventi memorizzati dati "personali", ovvero i sistemi di protezione minimi previsti dal Legislatore e richiesti a chiunque detenga dati relativi a terze persone, Aziende od Enti
- Sanzioni previste per gli inadempienti, ovvero per coloro che omettono di attivare un sistema di protezione dei dati – siano essi memorizzati in formato digitale o in qualunque altra forma – adeguato alla natura dei dati posseduti e comunque almeno ai requisiti minimi, e/o che non provvedano alla creazione e progressivo aggiornamento "documento programmatico della sicurezza"

Analisi dei punti salienti

Natura delle operazioni sulle operazioni sulle informazioni presenti presso gli Enti od Aziende oggetto della Normativa in argomento

Art. 4 lettera a)
La Normativa elenca minuziosamente le operazioni che possono essere compiute sulle informazioni – chiamate anche "dati" se all'interno di un sistema informativo -, tanto manualmente quanto con sistemi elettronici – computer in particolare -; in sostanza per "trattamento" viene considerata qualunque operazione eseguita sulle informazioni.

Natura dei dati oggetto della Normativa in argomento

Vengono di seguito analizzati i tipi di dati considerati dalla Normativa in argomento; ognuna delle categorie richiede interventi definiti come "minimi" sul proprio sistema di trattamento, ai quali devono essere affiancati interventi specifici in funzione della tipologia dei dati e dell'attività dell'Azienda od Ente che li detiene – la scopo della presente analisi non comprende considerazioni su tali interventi specifici, in quanto identificabili solo a fronte di un'analisi diretta delle singole realtà -.

Art. 4 lettera b) – Dati Personali
La definizione riporta espressamente l'allocuzione "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione"; queste informazioni sono considerate "personali" nel momento in cui in un modo qualunque – diretto, indiretto, codificato o meno - possono essere collegate al nominativo cui sono riferite. La Normativa non opera distinzioni tra i luoghi fisici od "informatici" presso i quali le informazioni ed i dati che ne permetterebbero l'attribuzione a persona fisica o legale sono appoggiati; di conseguenza la distanza – fisica o informatica – tra i luoghi di archiviazione non ha rilevanza ai fini del Decreto Legislativo.

Art. 4 lettera c) – Dati identificativi
Si intendono con questa accezione i dati che consentono di correlare i "Dati Personali" alle Persone ed Enti cui sono relativi; ad esempio, il numero di codice che permette di associare una determinata fattura al relativo Cliente

Art. 4 lettera d) – Dati sensibili
Si intendono con questa accezione i dati che per loro natura potrebbero essere causa di discriminazioni; tra gli altri, dati relativi alla vita ed ai gusti sessuali, al credo politico, alla religione professata, allo stato di salute e così via.
Si tratta nella sostanza di quei dati più comunemente considerati degni di protezione da parte della normativa sulla "privacy", costituenti una sotto-categoria dei "Dati Personali".

Art. 4 lettera e) – Dati giudiziari
Si intendono con questa accezione i dati utili a rivelare la condizione giudiziaria – presente, pregressa o in fase di definizione – di Persone fisiche e giuridiche.

Destinatari della nuova normativa

Destinatari della nuova normativa sono tutti coloro – Aziende ed Enti Pubblici – che detengano – in qualunque forma, elettronica e non - informazioni o dati personali – secondo la definizione sopra riportata - relativi a persone fisiche o giuridiche; recita infatti letteralmente la normativa - Art. 5 punto 1 - "Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato."

Appare dunque improbabile che un archivio – elettronico o meno - utilizzato per attività professionali possa non contenere dati personali; la sola presenza di una scheda relativa ad un Cliente o di un'agenda realizzata con un semplice foglio di calcolo fa ricadere l'intera rete dell'Azienda o dell'Ente nell'ambito di applicazione della normativa, così come una lettera recante l'indirizzo del destinatario.

Principali adempimenti

La normativa riporta una serie di indicazioni generali riguardo ai trattamenti minimi da realizzare, di cui ai punti successivi; riporta inoltre un dettagliato "Disciplinare tecnico in materia di misure minime di sicurezza", all'interno del quale vengono più in dettaglio descritta la natura di tali interventi minimi.

L'Art. 31 elenca quali siano le finalità primarie che i disposti del Decreto Legislativo devono garantire rispetto alle informazioni, ovvero:

- la massima riduzione dei rischi di distruzione o perdita; in questo caso deve essere creato un sistema di salvataggio che non si limiti ad una generica copia "una tantum"
- la massima riduzione dei rischi di intrusione di estranei non autorizzati tra i dati, tanto per la loro lettura, quanto per il loro utilizzo non consono ai dati stessi.

L'Art. 33 ribadisce l'obbligatorietà delle azioni di cui all'articolo 31, considerandole come il minimo intervento necessario – e come tale da eventualmente integrare con maggiori interventi in funzione della natura delle informazioni possedute -.

L'Art. 34 elenca quindi per grandi linee le misure di sicurezza minime da attuare in un sistema informativo, rimandando al "Disciplinare Tecnico" per i particolari.
Tali misure consistono nell'attivare:

- Un **sistema di autenticazione per l'accesso ai dati** – Si tratta della gestione dei codici di accesso – password o simili in particolare – alle macchine ed ai dati; tali password dovranno, secondo i dettami del "Disciplinare Tecnico", essere gestite in modo razionale da un Responsabile, periodicamente aggiornate, ideate secondo criteri di sicurezza – quindi non banalmente adottando date di nascita o nominativi di parenti –
- Procedure di **gestione delle credenziali di autenticazione**, ovvero sistemi tali da garantire l'effettiva motivazione all'accesso da parte degli autorizzati, ed il ritiro delle credenziali a chi non lo fosse ulteriormente
- L'**aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici**, ovvero un sistema di controllo dell'accesso ai dati da parte degli operatori addetti alla gestione e manutenzione dell'hardware
- La **protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici**; tale protezione si riferisce, in campo elettronico, ad esempio ai cosiddetti "worm" – programmi spia che, inserendosi nel sistema operativo, rendono accessibili i computer dall'esterno per via telematica -, ai virus informatici, agli attacchi da parte di hacker – i cosiddetti "pirati informatici -. In prima battuta si parla di programmi antivirus e di firewall, che devono essere correttamente installati, settati e regolarmente aggiornati
- L' **adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi**, ovvero non semplici copie pur fatte ad intervalli regolari, ma un sistema efficiente e completo per garantire l'integrità dei dati; un sistema di questo tipo deve ad esempio prevedere e giustificare le tecniche di salvataggio, la loro tempistica, i luoghi di custodia delle copie e così via.
- La **tenuta di un aggiornato documento programmatico sulla sicurezza**, ovvero di un documento all'interno del quale venga descritta e giustificata la politica di sicurezza adottata, le modalità di verifica e così via. Questo documento attesta la bontà delle azioni intraprese, la loro adeguatezza rispetto alla natura delle informazioni detenute, costituendo quindi il primo elemento di verifica da parte delle Autorità preposte agli accertamenti; deve quindi essere realizzato in modo coerente ed adeguato alla situazione in essere, completo in ogni sua parte, e soprattutto esaustivo per quanto riguarda la politica della sicurezza adottata.
- L' **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**, ovvero di tecniche avanzate di protezione applicate direttamente ai dati qualora siano presso l'Ente o l'Azienda dati cosiddetti "sensibili"

Regime sanzionatorio

L'Art. 169 è molto sintetico nella propria formulazione, prevedendo l'arresto fino a due anni, o in alternativa una sanzione da € 10.000 a € 50.000, oltre all'obbligo di adeguamento del proprio sistema entro un tempo di massimo sei mesi – fatte salve eventuali deroghe per motivi prettamente tecnici -.

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Legge delega n. 127/2003

Entrata in vigore dei disposti: Art. 186 (Entrata in vigore)
1. Le disposizioni di cui al presente codice entrano in vigore il 1° gennaio 2004, ad eccezione delle disposizioni di cui agli articoli 156, 176, commi 3, 4 5 e 6 e 182, che entrano in vigore il giorno successivo alla data di pubblicazione del presente codice. Dalla medesima data si osservano altresì i termini in materia di ricorsi di cui agli articoli 149, comma 8, e 150, comma 2.

Oggetto: Diritto di ciascuno alla protezione dei dati personali che lo riguardano – Titolo I Art. 1 –

Finalità: Art. 2
1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Definizioni: Art. 4
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;
….

Oggetto ed ambito di applicazione: Art. 5
1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.
2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

DOTAZIONI DI SICUREZZA MINIME: Titolo V

CAPO I MISURE DI SICUREZZA

Art. 31 (Obblighi di sicurezza)

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, 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.

Art. 33 (Misure minime)

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34 (Trattamenti con strumenti elettronici)

1. 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:
autenticazione informatica;
adozione di procedure di gestione delle credenziali di autenticazione;
utilizzazione di un sistema di autorizzazione;
aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
tenuta di un aggiornato documento programmatico sulla sicurezza;
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.

CAPO II – ILLECITI PENALI

Art. 169 (Misure di sicurezza)

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi.

…..

ALLEGATO B

DISCIPLINARE TECNICO
IN MATERIA DI MISURE MINIME DI SICUREZZA

(Artt. 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.