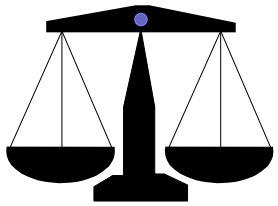
Azienda Ospedaliera di Verona
Servizio Sistemi Informativi

INTRODUZIONE AL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Decreto Legislativo 196/2003



La protezione dei dati personali – Normativa

- Direttiva 1995/46/CE
- Direttiva 2002/58/CE
- D.Lgs. 196/2003

La sfida cruciale sottesa alla normativa è la faticosa conciliazione tra il rispetto dei fondamentali diritti della persona, la libera trasmissione e circolazione delle informazioni e il bisogno di sicurezza.

Privacy = diritto

TRE DIRITTI FONDAMENTALI DELLA PERSONA:

- Diritto alla privacy
- Libera trasmissione e circolazione delle informazioni
- Bisogno di sicurezza

=> EQUILIBRIO!

Privacy = Responsabilità

- La conoscenza degli aspetti legali correlati alla sicurezza informatica è di fondamentale importanza per gli utenti del sistema informativo aziendale.

- Le nuove tecnologie hanno creato nuove responsabilità per gli operatori e le aziende ed hanno reso necessaria un'attenta analisi degli aspetti legali, che favorisca il raggiungimento degli obiettivi di efficienza nel rispetto della legislazione vigente.

Privacy e sicurezza

- Cosa si rischia se non si implementa la sicurezza in azienda? La risk analisys deve comprendere anche la risk analisys legale, troppo spesso dimenticata!
- Implementazione della sicurezza… anche al fine del raggiungimento della conformità alla legislazione!
- Sicurezza dei dati e dei sistemi:
  - Sicurezza fisica: protezione delle aree e dei locali; protezione della rete
  - Sicurezza logica: protezione della rete e dei sistemi
  - Sicurezza organizzativa: istruzioni, procedure di sicurezza

Il D.Lgs. 196/2003

- Fino al 31 dicembre 2003:
  - L. 31 dicembre 1996 n. 675 (e successive modificazioni ed integrazioni, in particolare introdotte dal D.Lgs. 467/2001)
  - D.P.R. 28 luglio 1999 n. 318
- Dal 1 gennaio 2004:
  - "Codice in materia di protezione dei dati personali", contenuto nel D.Lgs. N. 196 che unisce in un unico corpo normativo tutte le disposizioni in materia di *privacy*.

La struttura del codice

- Il nuovo Codice in materia di protezione dei dati personali è suddiviso in tre parti + allegati
  1. Disposizioni generali (settore pubblico e privato)
  2. Disposizioni relative a specifici settori (ambito giudiziario, forze di polizia, **settore sanitario**, …)
  3. Tutela dell'interessato e sanzioni
  4. [Allegati (A: Codici deontologici, B: Misure minime di sicurezza, C: Trattamenti non occasionali in ambito giudiziario o per fini di polizia)]
- Il Codice si applica a chiunque è stabilito nel territorio dello Stato, anche se i dati sono detenuti all'estero.

Alcune definizioni

FONTE	TERMINE	DEFINIZIONE
Art.4 c.1 lett.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;
Art.4 c.1 lett.c)	**Dati identificativi**	i dati personali che permettono l'identificazione diretta dell'interessato;
Art.4 c.1 lett.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;
Art.4 c.1 lett.e)	**Dati giudiziari**	i dati personali idonei a rivelare provvedimenti … 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 …

Alcune definizioni

FONTE	TERMINE	DEFINIZIONE
Art.4 c.1 lett.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;
Art.4 c.1 lett.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;
Art.4 c.1 lett.m)	diffusione	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Il principio di necessità – art. 3

- Chiunque ha diritto alla protezione dei dati personali che lo riguardano: SONO TUTELATE SIA LE PERSONE FISICHE CHE GIURIDICHE!
- PRINCIPIO DI NECESSITA': i sistemi ed i programmi informatici dovranno essere configurati in modo da **ridurre al minimo l'utilizzazione dei dati personali e identificativi. Sarà necessario escluderne l'uso se sussiste la possibilità di 1) rendere anonimo il dato; 2) identificare l'interessato solo in caso di necessità.**
- In concreto, ciò significa che il titolare del trattamento dovrà preventivamente adottare tutte le misure organizzative/informatiche necessarie per permettere l'accesso ai soli dati indispensabili all'attività lavorativa, addirittura anonimizzando i dati se possibile.

Il principio di necessità permea il Codice in ogni sua parte e il titolare del trattamento deve tenerlo in considerazione ogniqualvolta si trovi di fronte ad una scelta, sia essa di carattere organizzativo oppure tecnologico.

Altre definizioni: i soggetti

FONTE	TERMINE	DEFINIZIONE
Art.4 c.1 lett.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;
Art.4 c.1 lett.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;
Art.4 c.1 lett.h)	Incaricati	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
Art.4 c.1 lett.i)	Interessato	la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

I soggetti che effettuano il trattamento: il **titolare** (artt. 4+28)

- DEFINIZIONE ex art. 4:
  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;

- Art. 28: quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente,associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita <u>un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza</u>.

I soggetti che effettuano il trattamento: il **responsabile** (artt. 4+29)

- DEFINIZIONE ex art. 4:
  la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

  Art. 29:
- Il responsabile è designato dal titolare facoltativamente.
- Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
- I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.
- Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

I soggetti che effettuano il trattamento: gli **incaricati** (artt. 4+30)

- DEFINIZIONE ex art. 4:
  le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

  Art. 30:
- Gli incaricati operano sotto la diretta autorità del titolare o del responsabile e devono attenersi alle istruzioni impartite.
- La designazione deve essere effettuata per iscritto e deve individuare puntualmente l'ambito del trattamento consentito.
- La designazione è corretta anche documentando la preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità stessa.

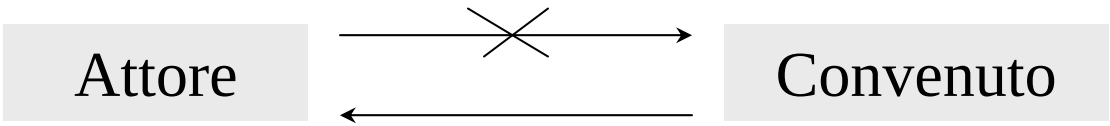
Alcune regole generali

- **<u>Diritto di accesso ai dati</u>** (art.7 e ss.): agevolare l'accesso ai dati personali da parte dell'interessato, semplificare le modalità e ridurre i tempi per il riscontro.
- **<u>Regole per il trattamento dei dati</u>** (art.11): liceità, correttezza, pertinenza agli scopi, esattezza, conservazione limitata nel tempo secondo le finalità dichiarate.
- **<u>Informativa</u>** (art. 13): può essere data anche oralmente o con un cartello e deve indicare
  - Finalità/modalità trattamento dati
  - Natura obbligatoria/facoltativa conferimento dati
  - Conseguenze eventuale rifiuto di rispondere
  - Coloro (siano anche responsabili o incaricati) ai quali i dati personali possono essere comunicati e ambito di diffusione
  - Diritti di cui all'art.7 (accesso)
  - Estremi del titolare/rappresentante territorio dello Stato/responsabile
- **<u>Consenso</u>** (art.23): deve essere libero, specifico, informato, documentato per iscritto. Se il trattamento riguarda *dati sensibili*, il consenso deve essere manifestato in *forma scritta*. **Le strutture sanitarie possono avvalersi di modalità semplificate** (art. 81: … può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anzichè con atto scritto dell'interessato, con annotazione dell'esercente la professione sanitaria …)

La responsabilità civile (art. 15)

- Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile (esercizio di attività pericolose), “se non prova di aver adottato tutte le <u>misure idonee ad evitare il danno</u>”
- Non esistono parametri minimi di valutazione dell’idoneità, se non il “progresso tecnico” e l’*importanza* dei dati trattati (art. 31)

INVERSIONE DELL’ONERE DELLA PROVA!



Art. 31

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

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.

NB: L'adozione delle misure minime (allegato B) ci mette al riparo dalla responsabilità penale ma non è detto che ci tuteli dal punto di vista della responsabilità civile (per la cui tutela devono essere adottate le misure idonee, come indicato nell'art.31).

Quali MISURE MINIME?

Art.34 – Trattamento 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:

a) **autenticazione informatica**;

b) adozione di **procedure di gestione delle credenziali** di autenticazione;

c) utilizzazione di un **sistema di autorizzazione**;

d) **aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati** e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) **protezione degli strumenti elettronici e dei dati** rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato **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.

Art.35 - Trattamento senza l'ausilio di strumenti elettronici

1. 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 della 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.

Autenticazione	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.

Il Disciplinare Tecnico – Allegato B

Parola chiave	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.
Sostituzione della parola chiave	5. 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.
User Id	6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
Verifica di sussistenza condizioni per autenticazione	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.

Il Disciplinare Tecnico – Allegato B

Disconnessione	9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
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.
Aggiornamento profili nel sistema di autorizzazione	14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
	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.

Il Disciplinare Tecnico – Allegato B

Virus	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.
Intrusione	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.
Patch (=> no w9x)	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.

Art.615-quinquies del Codice Penale
Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire 20 milioni

Art.615-ter del Codice Penale
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

Il Disciplinare Tecnico – Allegato B

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

Istruzioni agli incaricati	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.
	5. 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.
	9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Istruzioni agli incaricati	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.
	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.

Il Disciplinare Tecnico – Allegato B

D.P.S.	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 …
Attestazione di adozione D.P.S.	26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
Particolari accorgimenti	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.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Istruzioni agli incaricati per la custodia dei documenti contenenti dati personali	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.
Custodia dei documenti contenenti dati sensibili o giudiziari	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.
Accesso agli archivi fisici	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.

Tutela amministrativa e giurisdizionale (artt. 141 - 152)

- Amministrativa: davanti al Garante
  - Reclami
  - Segnalazioni
  - Ricorsi

- Giurisdizionale: davanti all'Autorità giudiziaria competente
  - Ricorso presentato alla cancelleria del Tribunale competente (quello dove risiede il titolare del trattamento)

Le sanzioni (artt. 161-172)

Violazioni amministrative

VIOLAZIONE	RIF.	SANZIONE
Omessa o inidonea informativa all'interessato (art. 161)	Artt. 13, 17, 26, 27	Da 3.000 a 18.000 Euro se dati personali. Da 5.000 a 30.000 Euro se dati sensibili. Aumento fino al triplo se inefficacia in ragione delle condizioni economiche dell'interessato. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Cessione di dati (art. 162 comma 1)	Art. 16	Da 5.000 a 30.000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Comunicazione dei dati all'interessato da parte di altri rispetto al medico designato dal titolare o dall'interessato (art. 162 comma 2)	Art. 84	Da 500 a 3.000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Omessa o incompleta notificazione (art. 163)	Artt. 37, 38	Da 10.000 a 60.000 Euro e pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Omessa informazione o esibizione al Garante (art. 164)	Artt. 150, 157	Da 4.000 a 24.000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.

Le sanzioni (artt. 161-172)

Violazioni penali

VIOLAZIONE	RIF.	SANZIONE
Trattamento illecito di dati (art. 167 comma 1) (tra gli altri, trattamento senza il consenso dell'interessato)	Artt. 18, 19, 23, 123, 126, 129, 130	Reclusione da 6 a 18 mesi. Se si tratta di comunicazione o diffusione di dati, da 6 a 24 mesi. Pubblicazione della sentenza.
Trattamento illecito di dati (art. 167 comma 2) (tra gli altri, violazione delle norme sui dati sensibili)	Artt. 17, 20, 21, 22, 25, 26, 27, 45	Reclusione da 1 a 3 anni. Pubblicazione della sentenza
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168)	Art. 37	Reclusione da 6 mesi a 3 anni. Pubblicazione della sentenza
Misure minime di sicurezza (art. 169)	Art. 33	Arresto fino a 2 anni o ammenda da 10.000 a 50.000 Euro. Prescrizione da parte del Garante che fissa un termine per la regolarizzazione (max 6 mesi). Se risulta l'adempimento della prescrizione del Garante, l'autore del reato è ammesso a pagare un quarto del massimo dell'ammenda stabilita. L'adempimento e il pagamento estinguono il reato.
Inosservanza di provvedimenti del Garante (art. 170)	Artt. 26, 90, 143, 150	Reclusione da 3 mesi a 2 anni. Pubblicazione della sentenza.
Violazione del divieto di indagine sulle opinioni dei lavoratori e del controllo a distanza (art. 171)	Artt. 113, 114	Arresto da 15 giorni a 1 anno o ammenda da 51 a 516 Euro. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente e la sentenza è pubblicata. Quando, per le condizioni economiche del reo l'ammenda può presumersi inefficace, il giudice ha facoltà di aumentarla fino al quintuplo.

Non si può prevedere tutto!!!