B

Misure minime di sicurezza

Disciplinare tecnico in materia di misure minime di sicurezza (*)

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.

……

ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI

Nel caso di trattamenti dei dati personali mediante l'accesso ad archivi cartacei o senza l'ausilio di strumenti elettronici:

a) l'accesso è consentito ai dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
b) se per il trattamento sono utilizzati atti e documenti contenenti dati personali, sensibili e giudiziari conservati in archivi ad accesso controllato, l'Incaricato deve osservare le regole e le procedure per l'accesso controllato, nonché proteggere tali fascicoli cartacei fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione;
c) i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere trattati mediante l'utilizzo meccanismi di cifratura, codici identificativi o altre soluzioni in modo che gli interessati siano identificati solo in caso di necessità e conservati separatamente dagli altri dati personali per finalità che non ne richiedono l'utilizzo

Nel caso di trattamenti dei dati personali con strumenti elettronici o comunque automatizzati:

a) se l'accesso ai dati è effettuato utilizzando un nome utente ed una parola chiave, l'Incaricato deve tenere le parole chiave strettamente riservate e cambiarle periodicamente alla scadenza secondo quanto previsto dall'Allegato B) del D.Lgs. 30 giugno n. 196, avendo l'accortezza di non utilizzare parole di senso compiuto che permetterebbero una semplice individuazione ed evitando in qualsiasi caso di annotarle su carta o in luoghi non sicuri;
b) se è necessario l'accesso di altre persone al suo PC, l'Incaricato non può rendere note le sue credenziali di accesso (username+password), ma è tenuto a predisporre un'altra modalità di accesso ai dati per chi deve operare su suoi files e per qualsiasi emergenza deve consegnare alla persona designata (Incaricato della custodia delle copie delle credenziali) una busta chiusa contenente la password;
c) se disponibile e compatibile con l'attività lavorativa, l'Incaricato deve registrare gli archivi trattati su una posizione prestabilita (ad esempio un disco di rete condiviso) di cui sia regolarmente effettuato il back-up. Qualora questa non sia disponibile o non si reputi opportuno utilizzarla, l'Incaricato è comunque tenuto ad assicurarsi che i dati vengano salvati con cadenza almeno settimanale e le copie riposte in luogo sicuro;
d) se si riscontra il mancato utilizzo delle credenziali d'accesso per un arco di tempo di almeno sei mesi, esse saranno disattivate e per ottenerne l'eventuale riattivazione l'Incaricato deve rivolgersi al Responsabile del trattamento dei dati;
e) tutti gli elaboratori, compatibilmente con il sistema operativo in uso, devono essere protetti da software antivirus da aggiornare con cadenza almeno semestrale o possibilmente impostato per l'aggiornamento automatico;
f) non è consentita, anche se possibile tecnicamente, l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro;
g) se non utilizzati e in ogni caso fuori dall'orario di lavoro l'Incaricato deve accertarsi di aver chiuso la sessione di lavoro ("log-off") in modo che siano richieste le credenziali di accesso al successivo utilizzo;
h) l'Incaricato deve custodire i supporti rimovibili sui quali sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti. Nel caso di trattamento dei dati sensibili o giudiziari, i supporti removibili già utilizzati per il trattamento possono essere riutilizzati per altro scopo solo se le informazioni in precedenza contenute siano completamente sovrascritte o rese tecnicamente inutilizzabili, altrimenti dovranno essere distrutti;
i) l'Incaricato deve adottare meccanismi di cifratura, codici identificativi o altre soluzioni per trattare i dati sensibili e giudiziari in modo che gli interessati siano identificati solo in caso di necessità. In particolar modo sono tenuto ad utilizzare detti meccanismi gli esercenti professioni sanitarie per trattare i dati inerenti lo stato di salute e la vita sessuale in modo disgiunto da quelli identificativi. L'Incaricato deve conservare i dati idonei a rivelare lo stato di salute e la vita sessuale separatamente dagli altri dati personali per finalità che non richiedono il loro utilizzo.
j) l'Incaricato è tenuto a trattare i dati genetici esclusivamente all'interno di locali protetti accessibili ai soggetti autorizzati ad accedervi, garantendo che il loro trasporto all'esterno dei locali riservati al trattamento avvenga in contenitori muniti di serratura e che il loro trasferimento in formato elettronico sia cifrato.

Definizioni utili:

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;

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

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

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 dati;

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

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 di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.