

**QUESTIONARIO PER LA VERIFICA DELLE MISURE “MINIME” DI SICUREZZA
PER LA PROTEZIONE DEL TRATTAMENTO DEI DATI EFFETTUATO CON
L'AUSILIO DI STRUMENTI ELETTRONICI**

1. Per l'accesso ai dati personali è previsto l'utilizzo di un sistema di autenticazione informatica, cioè vengono attribuite agli «incaricati» utenti del sistema informativo le cosiddette «credenziali di autenticazione» ?

SI NO ALTRO _____

2. In che cosa consistono le credenziali di autenticazione?

2.1 consistono in un codice di identificazione personale dell'incaricato (*user-id*), associato ad una *password* conosciuta soltanto dall'incaricato stesso?

SI NO ALTRO _____

2.2 consistono in un dispositivo di autenticazione (*smart card*) in possesso e uso esclusivo dell'incaricato, associato eventualmente ad un codice identificativo personale o ad una *password* segreta?

SI NO ALTRO _____

2.3 consistono in una caratteristica biometrica dell'incaricato , associata eventualmente ad un codice identificativo personale o ad una *password* segreta?

SI NO ALTRO _____

3. Prima che l'amministratore di sistema assegni la *password* iniziale a ciascun «incaricato» viene verificato che essa venga fornita individualmente ed esclusivamente a persone che hanno ricevuto una specifica lettera di nomina ad «incaricato del trattamento» e delle quali viene tenuto dall'ente titolare (*in particolare dal soggetto incaricato dall'ente di presidiare il rispetto della normativa sulla privacy*) un elenco nominativo aggiornato?

SI NO ALTRO _____

4. Sono state fornite agli «incaricati» delle adeguate istruzioni scritte per quanto riguarda le cautele da osservare per garantire la segretezza della loro *password* personale e per garantire la diligente custodia degli eventuali dispositivi di autenticazione (*ad es. le smart card*) in loro possesso ed uso esclusivo?

SI NO ALTRO _____

5. Sono stati nominati per iscritto i soggetti «incaricati della custodia delle parole chiave» oppure i soggetti che hanno comunque accesso ad informazioni che concernono le *password*?

SI NO ALTRO _____

6. Sono state date agli «incaricati» specifiche istruzioni affinché essi provvedano autonomamente alla sostituzione della *password* segreta almeno ogni 6 mesi (oppure minimo ogni 3 mesi se l'incaricato tratta dati «sensibili» o «giudiziari»)?

SI NO ALTRO _____

7. Ogni volta che un «incaricato» provvede all'autonoma sostituzione della sua *password* segreta, la comunica in una busta chiusa alla persona nominata «incaricato della custodia delle parole chiave»?

SI NO ALTRO _____

8. In alternativa, quale altra procedura viene adottata aziendaliamente per custodire le *password* e mantenere la loro segretezza?

SI NO ALTRO _____

9. Viene verificato che i codici per l'identificazione personale degli incaricati (*user-id*) non vengano mai assegnati a diversi incaricati, neppure in tempi diversi?

SI NO ALTRO _____

10. Prima del rilascio dello *user-id* ad un «incaricato del trattamento» viene accertato che il richiedente ne abbia l'effettiva necessità per poter adempiere ai compiti a lui assegnati dal titolare (*cioè viene verificato il «need to know», tenendo presente che vi è una sostanziale differenza tra ciò che l'incaricato può conoscere e ciò che deve conoscere*)?

SI NO ALTRO _____

11. In caso di perdita del «*need to know*» (*cioè di perdita della qualità che consente all'incaricato l'accesso a determinati dati personali che egli «deve» conoscere*) è prevista la disattivazione immediata del suo *user-id*?

SI NO ALTRO _____

12. È prevista la disattivazione dello *user-id* dopo 6 mesi di suo mancato utilizzo da parte di un «incaricato» (salvo che per le *user-id* preventivamente autorizzate per i soli scopi di gestione tecnica del sistema informativo)?

SI NO ALTRO _____

13. Sono state impartite delle precise istruzioni scritte agli «incaricati» di non lasciare incustodito e accessibile durante una sessione di lavoro (*cioè informaticamente «aperto»*) l'elaboratore elettronico a loro affidato per il trattamento dei dati?

SI NO ALTRO _____

14. Sono state impartite idonee e preventive disposizioni scritte (*cioè delle procedure da inserire nell'eventuale «Manuale della privacy» aziendale*) con le quali sono state individuate le modalità attraverso le quali il «titolare del trattamento» può accedere ai dati o agli elaboratori elettronici, nel caso di una prolungata assenza degli incaricati o di un loro impedimento, ma solamente per indispensabili ed indifferibili necessità di intervento, esclusivamente per necessità di operatività e di sicurezza del sistema informativo?

SI NO ALTRO _____

15. Sono stati individuati e configurati, prima dell'inizio del trattamento, dei profili di autorizzazione di ambito diverso per ciascun «incaricato» o per classi omogenee di incaricati (*i cosiddetti «privilegi» di accesso*), in modo che sia limitato il loro accesso ai soli dati necessari per effettuare il trattamento loro affidato?

SI NO ALTRO _____

16. Viene definito con precisione dall'ente titolare del trattamento, prima dell'inizio di un trattamento di dati personali con l'ausilio di strumenti elettronici, il profilo di autorizzazione di colui il quale è autorizzato all'accesso a tali dati (*cioè il profilo dello specifico singolo «incaricato del trattamento» viene definito preventivamente*)?

SI NO ALTRO _____

17. Viene controllata periodicamente (*e comunque almeno una volta all'anno*) la sussistenza in capo agli «incaricati» delle condizioni per la conservazione dei rispettivi profili di autorizzazione, ossia viene verificato periodicamente l'ambito di trattamento consentito ai singoli «incaricati» o alle classi omogenee di incaricati?

SI NO ALTRO _____

18. Viene controllato periodicamente (*e comunque almeno una volta l'anno*) l'ambito di trattamento consentito agli addetti alla gestione o alla manutenzione del sistema informativo?

SI NO ALTRO _____

19. I dati personali contenuti negli elaboratori elettronici sono stati adeguatamente protetti contro i rischi di intrusione e contro il software pericoloso mediante degli idonei programmi antivirus?

SI NO ALTRO _____

20. Viene verificata periodicamente l'efficacia (*con dei test di verifica o penetration test*) dei programmi antivirus e dei programmi contro il software pericoloso?

SI NO ALTRO _____

21. I programmi antivirus e i programmi contro il software pericoloso vengono aggiornati almeno ogni 6 mesi?

SI NO ALTRO _____

22. Viene effettuato almeno una volta all'anno (ovvero almeno ogni 6 mesi, se vengono trattati dati «sensibili» o «giudiziari») l'aggiornamento dei programmi per prevenire la vulnerabilità degli elaboratori elettronici e per correggerne i difetti ? (*patch o programmi update*)

SI NO ALTRO _____

23. Sono state impartite agli «incaricati» delle istruzioni organizzative e tecniche, preferibilmente per iscritto, che prevedono il salvataggio dei dati (*backup*) con una frequenza almeno settimanale?

SI NO ALTRO _____

24. Prima di consentire l'accesso ai dati «sensibili» o «giudiziari» contenuti nell'elaboratore, viene verificato che l'incaricato del trattamento (o il gruppo omogeneo di «incaricati» a cui egli appartiene), oppure l'addetto alla manutenzione del sistema informativo, abbia ricevuto una specifica autorizzazione ad accedere a questo tipo di dati (*cioè si configura il cosiddetto «incaricato autorizzato»*)?

SI NO ALTRO _____

25. Viene verificato che l'autorizzazione di cui al punto precedente sia stata rilasciata solamente da parte del «titolare» o da parte di una persona nominata «responsabile» dall'ente?

SI NO ALTRO _____

26. Viene verificato che l'autorizzazione rilasciata agli «incaricati del trattamento» o agli addetti alla manutenzione del sistema informativo, limiti il loro accesso ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione ad essi affidate?

SI NO ALTRO _____

27. Viene verificata la validità della richiesta di accesso a determinati dati personali prima di consentire l'accesso stesso ad un «incaricato del trattamento» ?

SI NO ALTRO _____

28. I supporti informatici rimovibili (*floppy disk, compact disc, nastri, cassette di backup*) che contengono dati «sensibili» o «giudiziari», se non vengono più utilizzati, vengono distrutti fisicamente o vengono comunque resi inutilizzabili?

SI NO ALTRO _____

29. Se i supporti informatici rimovibili già utilizzati per trattare dati «sensibili» o «giudiziari» non vengono distrutti, vengono riutilizzati soltanto se è del tutto esclusa la possibilità tecnica di recuperare le informazioni precedentemente contenute in essi?

SI NO ALTRO _____

30. Vengono impartite agli «incaricati» istruzioni tecniche ed organizzative, preferibilmente scritte, per la custodia e l'uso dei supporti rimovibili in cui sono memorizzati dati «sensibili» o «giudiziari», in modo da non consentire l'accesso non autorizzato a tali dati o il loro trattamento non consentito?

SI NO ALTRO _____

31. Vengono adottate idonee misure per garantire il ripristino dell'accesso ai dati «sensibili» o «giudiziari» in caso di danneggiamento degli stessi o degli strumenti elettronici con cui vengono trattati, in tempi certi compatibili con i diritti degli interessati e, comunque, al massimo entro 7

giorni?

SI NO ALTRO _____

32. Nel caso in cui l'ente tratti dati «sensibili» o «giudiziari» con l'ausilio di qualunque tipo di strumento elettronico, ha provveduto a redigere entro il 31 dicembre 2005 il nuovo DPS (Documento programmatico sulla sicurezza)?

SI NO ALTRO _____

33. L'ente tenuta alla redazione del DPS si ricorda che dovrà farne menzione nella relazione accompagnatoria al suo bilancio di esercizio 2005 (se l'ente è tenuta a farlo ai sensi dell'art. 2423 c.c.)?

SI NO ALTRO _____

34. L'ente è a conoscenza del fatto che il DPS dev'essere aggiornato entro il 31 marzo di ogni anno, e che si deve riferire di avere compiuto tale adempimento nella relazione accompagnatoria al bilancio di esercizio dell'ente di ogni anno?

SI NO ALTRO _____

35. Il Documento programmatico sulla sicurezza redatto dal titolare del trattamento contiene tutti gli elementi che sono previsti obbligatoriamente dal punto 19 del Disciplinare tecnico, allegato B) al D.Lgs. n. 196/2003?

SI NO ALTRO _____

36. In particolare, il DPS contiene gli elementi elencati nei punti seguenti, che riguardano il trattamento dei dati «sensibili» o «giudiziari» effettuato dall'ente titolare del trattamento? *(N.B. L'obbligo di fare il DPS riguarda solo chi tratta dati «sensibili» e «giudiziari» con l'ausilio di qualunque strumento elettronico e si riferisce in particolare al trattamento di tali dati personali, ma è opportuno descrivere nel DPS anche ciò che riguarda i dati comuni ed è consigliabile redigere comunque il DPS anche se si trattano solamente dati comuni).*

L'elenco dei trattamenti di dati effettuati?

SI NO ALTRO _____

La distribuzione dei compiti?

SI NO ALTRO _____

L'attribuzione delle responsabilità ?

SI NO ALTRO _____

L'analisi dei rischi che incombono sui dati trattati?

SI NO ALTRO _____

Le misure da adottare per garantire l'integrità e la disponibilità dei dati?

SI NO ALTRO _____

Le misure da adottare per garantire la protezione delle aree e dei locali in cui avviene il trattamento dei dati, che siano rilevanti per quanto riguarda la custodia e l'accessibilità dei dati stessi?

SI NO ALTRO _____

La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati «sensibili» o «giudiziari» distrutti o danneggiati, in tempi certi, compatibili con l'esercizio dei diritti degli interessati e comunque non superiori a 7 giorni?

SI NO ALTRO _____

La previsione di interventi formativi degli incaricati, per renderli edotti e consapevoli dei rischi che incombono sui dati e delle misure per prevenire i danni, nonché degli aspetti più rilevanti della normativa sulla privacy e delle responsabilità che derivano dal trattamento dei dati e infine delle modalità per aggiornarsi sulle misure minime di sicurezza adottate dal «titolare» ?

SI NO ALTRO _____

Solamente per gli organismi sanitari e per gli esercenti le professioni sanitarie:

L'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale - contenuti in elenchi, registri o banche dati (informatiche) - dagli altri dati personali dell'interessato?

SI NO ALTRO _____

Data e firma dell'incaricato del trattamento