Allegato “B 3“ – Misure minime di sicurezza per la protezione dei dati personali

MISURE MINIME DI SICUREZZA

Premessa

I dati personali oggetto di trattamento devono essere custoditi e controllati, adottando misure di sicurezza idonee che minimizzino i rischi di distruzione e perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito ovvero non conforme alle finalità previste.

Il decreto Legislativo n. 196/2003 richiede misure di sicurezza volte ad assicurare un livello minimo di protezione dei dati personali, come succintamente descritte nei paragrafi successivi.

Trattamento con strumenti elettronici

Nel caso in cui il trattamento dei dati personali avvenga utilizzando strumenti elettronici sono necessari degli adempimenti che:

- garantiscono l‘accesso ai dati solo agli incaricati autorizzati e con il profilo di autorizzazione previsto;
- non permettono un trattamento dei dati non conforme alle finalità;
- riducono al minimo i rischi di distruzione o perdita anche accidentali.

Gestione delle credenziali di autenticazione

Gli incaricati devono essere dotati di credenziali di autenticazione idonee a garantire l‘accesso ai trattamenti di competenza. Dette credenziali consistono in un codice per l‘identificazione (user-name) associato ad una parola chiave riservata (password) conosciuta esclusivamente dall‘incaricato.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Vengono disattivate anche in caso di perdita della qualità che consente all‘incaricato l‘accesso ai dati personali.

La parola chiave (password) deve essere composta da almeno otto caratteri, non deve contenere riferimenti agevolmente riconducibili all‘incaricato, deve essere modificata al primo utilizzo e, successivamente, ogni sei mesi. In caso di trattamento di dati sensibili e giudiziari la parola chiave è modificata almeno ogni tre mesi.

Autorizzazioni

I profili di autorizzazione 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.

Altre misure di sicurezza

In sede di individuazione dell‘ambito del trattamento consentito ai singoli incaricati e agli addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati puö essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

I dati personali sono protetti contro il rischio di intrusione mediante l‘attivazione di idonei strumenti elettronici (anti-virus) aggiornati con cadenza almeno semestrale.

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.

Istruzioni per gli Incaricati del trattamento

Le istruzioni agli incaricati contengono obbligatoriamente:

- cautele da adottare per assicurare la segretezza dei dati trattati e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell‘incaricato;
- istruzioni per non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento;
- modalità con le quali viene assicurata 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;
- istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con cadenza almeno settimanale;
- 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;

Ulteriori misure di sicurezza in caso di trattamento di dati sensibili e/o giudiziari

I dati sensibili o giudiziari richiedono ulteriori misure di sicurezza; in particolare:

- i supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili;
- il trattamento dei dati sanitari è effettuato con particolari tecniche (cifratura), come da art. 22 comma 6 del D. Lgs. n. 196/2003.

Trattamento senza l‘ausilio di strumenti elettronici

Nel caso di trattamento dei dati senza l‘ausilio di strumenti elettronici, sono previste le seguenti regole:

- 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;

- in sede di individuazione dell‘ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati puö essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;
- 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;
- 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.

P.S. Per la definizione dei termini usati, si rinvia all‘articolo 4 del D.Lgs. n. 196/2003 (codice in materia di protezione dei dati personali)

IL DIRETTORE GENERALE
Titolare del Trattamento
Dott. Carlo MIRABELLA