



Disciplinare Tecnico in Materia di Misure Minime di Sicurezza 2017

DISCIPLINARE TECNICO
IN MATERIA DI MISURE MINIME DI SICUREZZA
ANNO 2017



**Approvato dall'Amministratore Unico di Metro
con determina n. 2 del 24 gennaio 2017**



Sommario

Premessa	pag. 3
Trattamenti con strumenti elettronici	pag. 3
1) Allocazione del server	pag. 3
2) Utilizzo del personal computer e di altre apparecchiature e sistemi elettronici	pag. 3
3) Sistema di autenticazione informatica	pag. 3
4) Sistema di autorizzazione	pag. 4
5) Altre misure di sicurezza	pag. 5
6) Ulteriori misure in caso di trattamento di dati sensibili o giudiziari	pag. 5
7) Misure di tutela e garanzia	pag. 5
Trattamenti senza l'ausilio di strumenti elettronici	pag. 6
1) 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	pag. 6
Allegati	pag. 7
Allegato 1: Elenco dei server e dei database	pag. 7
Allegato 2: Elenco incaricati del trattamento	pag. 7
Allegato 3: Trattamento in outsourcing	pag. 7
Allegato 4: Piantine dei locali	pag. 7



Disciplinare tecnico 2017 in materia di misure minime di sicurezza

(ai sensi e per gli effetti degli artt. 31 e 33 del d.lgs. 196/2003, con particolare riferimento all'Allegato B del Decreto Legislativo a seguito delle abrogazioni avvenute con D.L. n.5/2012 e delle modifiche apportate con d.lgs. 28 maggio 2012, n.69)

Premessa

Il decreto legge 9 febbraio 2012 n. 5, convertito nella legge 4 aprile 2012 n. 35, e il decreto legislativo 28 maggio 2012 n. 69 hanno apportato abrogazioni e modifiche al decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali".

Per quanto sopra, non essendo più obbligatorio predisporre il "Documento programmatico sulla sicurezza", si è reso necessario operare secondo quanto disposto dal "Disciplinare tecnico in materia di misure minime di sicurezza" (Allegato B al decreto legislativo 196/2003).

Trattamenti con strumenti elettronici

1) Allocazione dei server

La Società dispone di due server. Uno è allocato presso la sede centrale, l'altro presso la sede dell'ufficio permessi.

I sistemi operativi sono in ambiente Windows e, in specifico, sono presenti: Windows Small Business Server 2011 Standard nella sede centrale e Windows Server 2008 R2 Standard all'ufficio permessi.

2) Utilizzo del personal computer e di altre apparecchiature e sistemi elettronici

L'utilizzo del personal computer, dei telefoni mobili e fissi e di altre apparecchiature e sistemi elettronici è regolato dal Codice di Comportamento Aziendale 2017 e dal Regolamento Interno del Personale 2017 che, oltre a stabilire regole comportamentali certe e vincolanti finalizzate a prevenire possibili abusi connessi all'utilizzo improprio di dette apparecchiature e sistemi, sono finalizzati ad un corretto utilizzo di tali strumenti al fine di prevenire trattamenti di dati difformi dalla legge.

Copia del Codice di Comportamento e del Regolamento Interno è stata consegnata a tutti i dipendenti.

3) Sistema di autenticazione informatica

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.

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 dispo-



tivo 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.

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

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.

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.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

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

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 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.

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.

4) Sistema di autorizzazione

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

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.

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.



5) Altre misure di sicurezza

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.

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.

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.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

6) Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

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.

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.

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.

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.

7) Misure di tutela e garanzia

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.



Trattamenti senza l'ausilio di strumenti elettronici

1) 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

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.

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.



Allegati

Gli allegati sotto elencati, i cui contenuti sono riservati e risultano agli atti di Metro Srl, sono parte integrante di questo documento.

Allegato 1: Elenco dei server e dei database

Allegato 2: Elenco incaricati del trattamento

Allegato 3: Trattamento in outsourcing

Allegato 4: Piantine dei locali