

dr. Marcello Polacchini
consulente aziendale

NON C'È PIÙ IL DPS... IL ROVESCIO DELLA MEDAGLIA



Copyright 2012 ©

**Il decreto legge 9 febbraio
2012 n. 5 - il cosiddetto
“decreto semplificazioni” del
Governo Monti - ha tra l’altro
abolito l’obbligo del DPS
(Documento Programmatico sulla
Sicurezza per il trattamento dei dati)**

Dopo anni di travagliata esistenza è venuto a mancare il

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA



Ne danno il triste annuncio il Garante per la protezione dei dati personali, i consulenti privacy, i cittadini interessati alla protezione e alla riservatezza dei loro dati personali.

I funerali si svolgeranno a Roma in Parlamento, non appena il decreto legge n. 5 approvato dal Consiglio dei Ministri il 9 febbraio 2012 sarà convertito in legge.

Non fiori, ma applicazione di tutte le misure di sicurezza necessarie per il trattamento dei dati e il rispetto della privacy dei cittadini.

30 giugno 2003

9 febbraio 2012

Il DPS è morto!



E adesso che cosa succederà...?

Tutti i titolari del trattamento di dati e specialmente le imprese hanno salutato con favore questa “semplificazione”, ma che cosa è cambiato?

Nella “sostanza” non è cambiato nulla!

Infatti, sono rimaste in vigore tutte le misure minime di sicurezza obbligatorie previste dal Codice della privacy e i provvedimenti generali del Garante che hanno effetto di legge.

**Da un certo punto di vista, l'aver
abolito il DPS è stata una cosa
positiva...**

**perché molti titolari del trattamento
di dati avevano identificato la
privacy con il DPS, facendo
prevalere l'obbligo di descrivere le
misure di sicurezza in un documento
sull'obbligo di adottarle
concretamente**

**Da un altro punto di vista però,
l'aver abolito il DPS è stata una
cosa negativa...**

**perché si trattava della misura di
sicurezza che consentiva ai titolari
del trattamento di tenere sotto
controllo il proprio sistema di
sicurezza per il trattamento dei
dati personali**

Molti non hanno capito che...

**Rispettare la privacy NON
significa redigere il DPS !**

**Però il DPS era uno strumento utile
specialmente per il titolare che
poteva ricordare ciò che aveva fatto
e quello che doveva ancora fare, e
poteva facilmente dimostrarlo in caso
di controlli o contestazioni**

**L'eliminazione del DPS ha
un rovescio della medaglia
che molti titolari del
trattamento di dati
rischiano di dimenticare
(specie le imprese e le
pubbliche amministrazioni)**

Infatti, senza il DPS le cose sono più complicate.

Perché il titolare deve comunque rispettare le REGOLE del Codice e deve compiere delle VERIFICHE periodiche sul proprio sistema di sicurezza per il trattamento dei dati personali.

Vediamo
brevemente quali
sono queste
REGOLE e queste
VERIFICHE...

**Ogni titolare del trattamento deve
rispettare i principi fondamentali
stabiliti dal decreto 196/2003:**

- **Pertinenza e non eccedenza dei
dati raccolti e trattati**
- **Esattezza dei dati e loro
eventuale aggiornamento**
- **Conservazione per un tempo non
superiore a quello necessario**

Inoltre, ogni titolare del trattamento ha una serie di **OBBLIGHI verso l'esterno (verso gli interessati) e all'interno della propria struttura organizzativa**

Il titolare del trattamento deve:

1. **Nominare le “figure privacy” e fornire loro adeguate istruzioni per il trattamento**
2. **Applicare tutte le misure “minime” di sicurezza previste dal Codice**
3. **Applicare le eventuali misure “idonee” di sicurezza che ritenesse necessarie**

4. Dare sempre una **informativa** agli interessati e ottenere il loro **consenso** (quando è necessario)
5. Garantire all'interessato il tempestivo **esercizio di tutti i diritti** riconosciutigli dall'art. 7
6. Se del caso, applicare i provvedimenti generali del Garante sugli **amministratori di sistema e sulla videosorveglianza**

7. **Verificare costantemente l'efficacia e l'efficienza del proprio Sistema di sicurezza per il trattamento dei dati personali, aggiornandolo quando è necessario o è previsto dalla legge**
8. **Dotarsi di una organizzazione interna efficace e mantenerla nel tempo**

**Perciò, oltre a osservare i
principi generali del Codice
della privacy, ogni titolare
deve rispettare sempre
alcuni adempimenti
obbligatoriosi**

Vediamoli...

1

INFORMATIVA

- **E' sempre necessaria e deve essere data solo alle persone fisiche**
- **Deve essere completa di tutti gli elementi indicati dall'art. 13**
- **Può non contenere gli elementi già noti agli interessati.**
- **Non deve essere rinnovata se non cambiano i suoi contenuti.**
- **Può essere data anche verbalmente**

2

CONSENSO

Di norma è necessario salvo che non si rientri nei casi di esclusione (previsti dall'art. 24 per i dati comuni e dall'art. 26 per i dati sensibili)

Il consenso non è più necessario per trattare i dati delle persone giuridiche

3

Nomina degli INCARICATI

- **La nomina è indispensabile e va fatta sempre per iscritto**
- **Devono essere fornite adeguate istruzioni per il trattamento dei dati (anche verbalmente)**
- **Sarebbe meglio fare della formazione specifica per gli incaricati del trattamento dei dati**

L'incaricato del trattamento è una figura fondamentale!

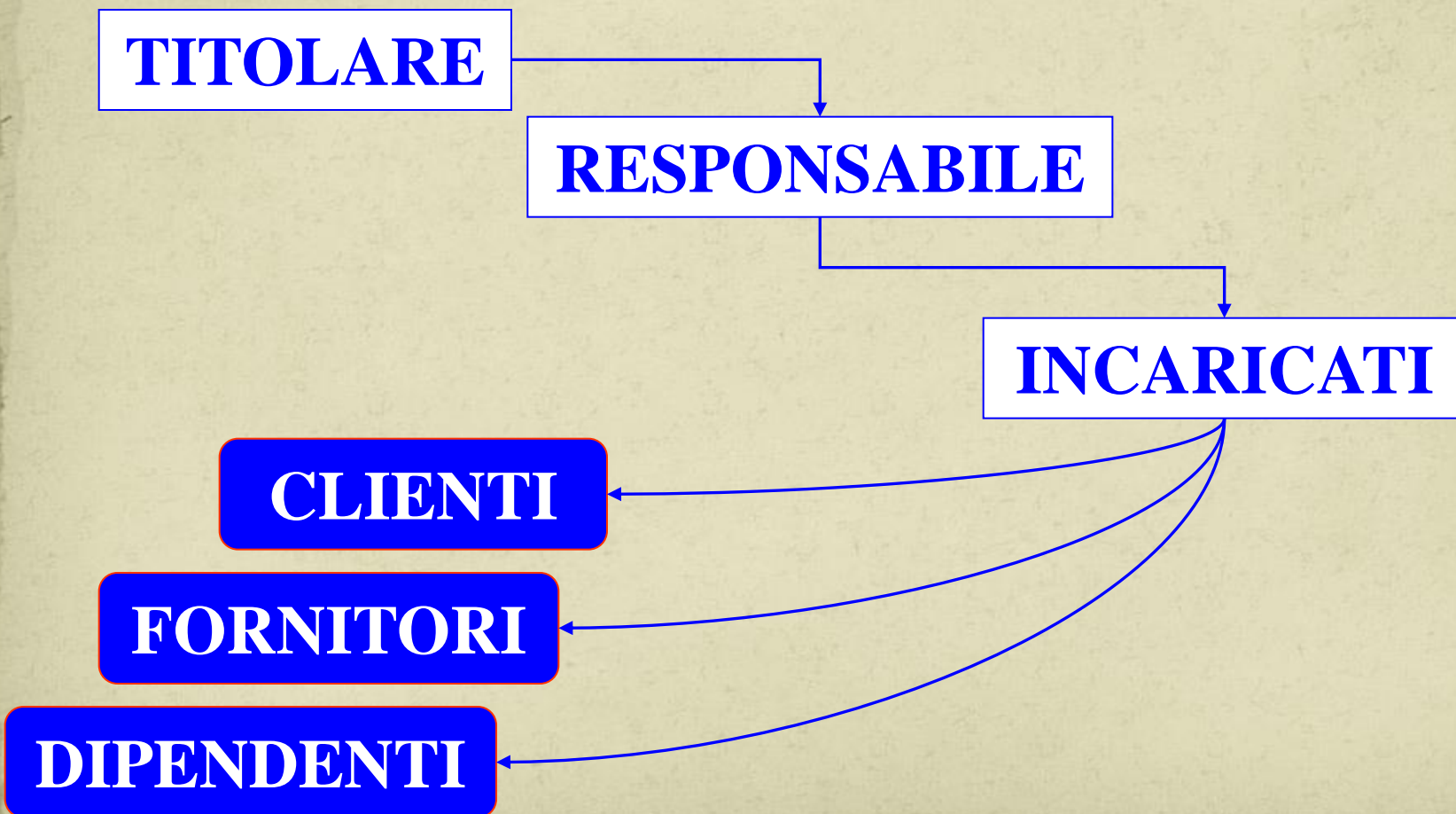
Perché la “PRIVACY” è soprattutto una questione di approccio mentale e comportamentale di ciascun incaricato del trattamento dei dati:

→ verso i DATI PERSONALI che tratta

→ verso la SICUREZZA del trattamento

Perciò, la “privacy” dipende prima di tutto da come l'incaricato si comporta rispetto a tutte le informazioni di cui viene a conoscenza durante il suo lavoro quotidiano.

L'elemento fondamentale della catena della sicurezza dei dati personali è **l'INCARICATO DEL TRATTAMENTO** cioè il soggetto che viene a contatto con le informazioni e deve trattarle in maniera corretta, rispettando le regole stabilite per la tutela della riservatezza.



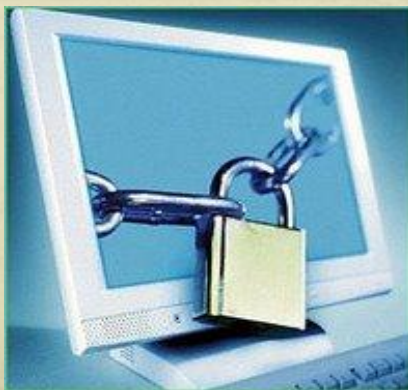
4

MISURE DI SICUREZZA

**Per il rispetto della
privacy sono
indispensabili le misure di
sicurezza per la
protezione dei dati
personali**

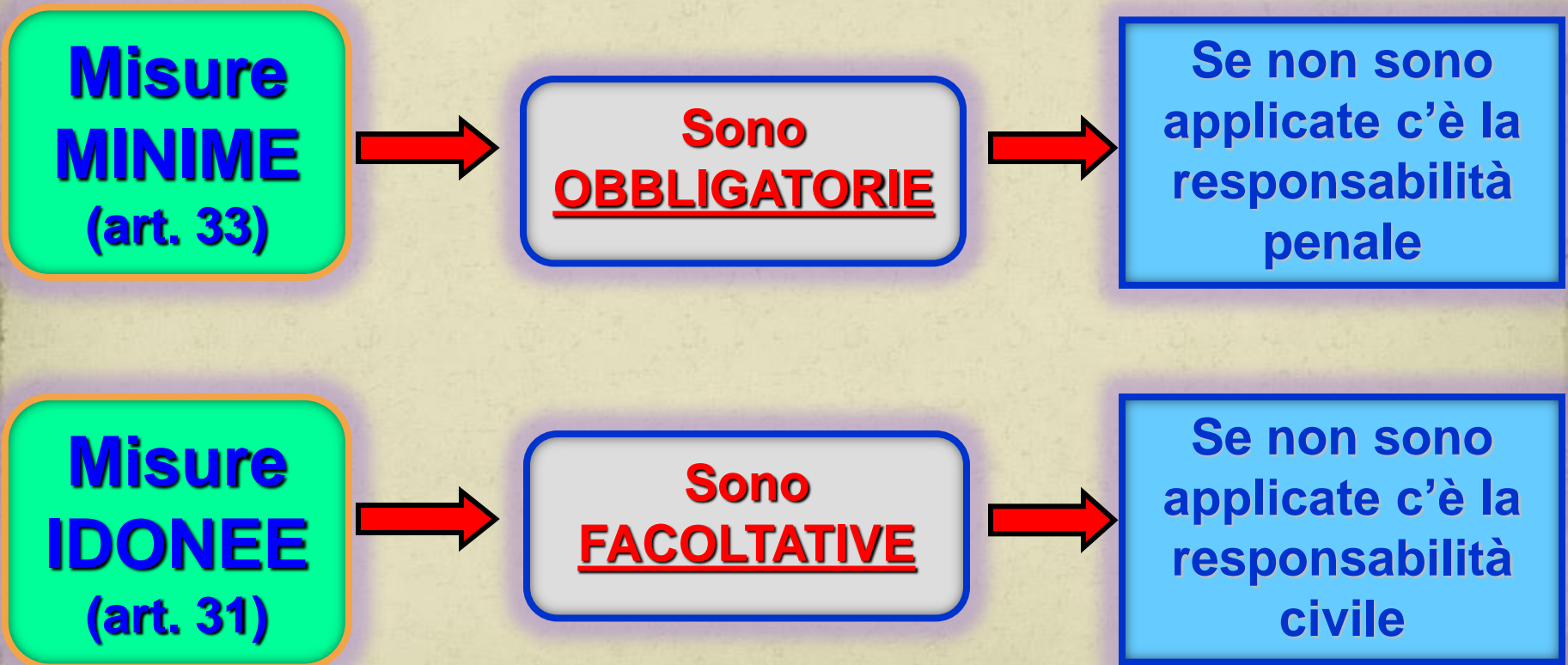
**Infatti, una cosa della quale
molti titolari del
trattamento non si rendono
ancora conto è che**

« Non c'è PRIVACY senza SICUREZZA »

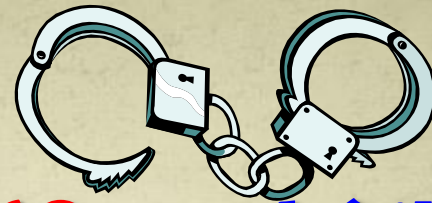


BISOGNA FARE ATTENZIONE
perché la mancata osservanza
delle disposizioni del Codice della
privacy può comportare
conseguenze molto pesanti per il
titolare, sia sul piano civile
(risarcimento dei danni), sia sul
piano penale e amministrativo
(sanzioni)

Ricordiamo che ci sono 2 tipi di misure di sicurezza...



E RICORDIAMO SEMPRE CHE...



Basta un comportamento COLPOSO perché il titolare possa essere condannato ai sensi dell'art. 169 del Codice.

Perciò, basta la semplice IGNORANZA della legge, ovvero la IMPRUDENZA o la IMPERIZIA di un incaricato del trattamento, oppure una NEGLIGENZA nell'applicazione delle misure minime di sicurezza, per fare scattare il reato penale nei confronti del titolare.

**Perciò, si devono rispettare gli
articoli 34 e 35 del Codice che
indicano che COSA FARE e
soprattutto si deve osservare il
Disciplinare Tecnico allegato al
Codice, che specifica COME FARE !**

La Legge sulla privacy costringe chiunque tratta dati a riflettere sui **RISCHI** che corre utilizzando le informazioni.

Perciò, è necessario che ogni titolare rifletta sul guadagno di **EFFICACIA** e di **EFFICIENZA** che può ottenere con un trattamento più **ORDINATO** e più **SICURO** di tutto il suo “patrimonio informativo”.

Da questa riflessione deve scaturire un vero e proprio ***“Sistema di sicurezza per il trattamento dei dati”***

Questo ***Sistema*** deve garantire il rispetto della normativa sulla privacy e può anche servire ad assicurare una migliore gestione di tutto il patrimonio informativo

**Oltre a tutto questo
il titolare del
trattamento di dati
deve anche
compiere delle
verifiche periodiche**

1

Deve verificare annualmente:

- **Le autorizzazioni concesse agli incaricati per l'accesso ai dati**
- **Le operazioni di trattamento dei dati consentite ai singoli incaricati**

2

Deve verificare semestralmente:

- **L'aggiornamento dell'antivirus**
- **L'aggiornamento dei programmi informatici (se tratta dati sensibili)**

CONCLUSIONE

Da tutto quello che ho detto è evidente che le cose da tenere sotto controllo sono molte e che l'abolizione del DPS non ha sicuramente aiutato il titolare in questo compito

Perciò, il consiglio per una corretta gestione dei rischi derivanti dal trattamento dei dati personali è di continuare a redigere un documento interno che descriva il proprio *Sistema di sicurezza per il trattamento dei dati*, indicando tutte le cose fatte e quelle ancora da fare

Così facendo il titolare del trattamento sarà in grado di dimostrare più agevolmente il rispetto della privacy e sarà preparato all'avvento del nuovo Regolamento UE che stabilirà regole ancora più stringenti e valide in tutta Europa

dr. Marcello Polacchini
consulente aziendale

**Vi ringrazio per
l'attenzione**