STEFANELLI & STEFANELLI STUDIO LEGALE

Regolamento 679/2016

il nuovo regime sanzionatorio
analisi del rischio e valutazione di impatto

avv. silvia stefanelli

DIR 95/46/CEE

…….l'obbligo di rispettare le regole fissate per la liceità dei trattamenti (art. 6) e solo come ulteriore dovere specifico quello di assicurare le misure di sicurezza adeguate

REGOLAMENTO UE

..nel Regolamento il Controller ha invece un ruolo proattivo, finalizzato non solo al rispetto delle regole ma anche alla necessità di dimostrare che ha adottato tutti gli accorgimenti tecnici e organizzativi necessari a garantire la "compliance" dei trattamenti

si passa da una disciplina di "adempimenti"

ad una disciplina di natura molto più sostanziale
(raggiungimento dell'obiettivo)

(legge 231/2001, Legge 190/2012)

PRINCIPI GENERALI DEL TRATTAMENTO (CAPO II)

ACCOUNTABILITY

ART. 5 comma 2

Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione")

Sanzioni art. 83

Articolo 24
Responsabilità del titolare del trattamento

Tenuto conto

- **della natura,**
- **dell'ambito di applicazione,**
- **del contesto e**
- **delle finalità del trattamento, nonché**
- **dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche**

il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento**

PROTEZIONE DEI DATI

ART. 32 - sicurezza del trattamento

Tenendo conto

- **dello stato dell'arte e**
- **dei costi di attuazione, nonché**
- **della natura,**
- **dell'oggetto,**
- **del contesto e**
- **delle finalità del trattamento, come anche**
- **del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche,**

il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative ADEGUATE** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

REGIMI SANZIONATORI

DIRITTO AL RISARCIMENTO DANNI

SANZIONI AMMINISTRATIVE

DIRITTO AL RISARCIMENTO DEL DANNO

Articolo 82
Diritto al risarcimento e responsabilità

1. *Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno* ***dal titolare del trattamento*** *o dal* ***responsabile del trattamento.***

*3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 s****e dimostra che l'evento dannoso non gli è in alcun modo imputabile.***

ONERE DELLA PROVA

DIRITTO AL RISARCIMENTO DEL DANNO

Articolo 82
Diritto al risarcimento e responsabilità

*Qualora **più titolari del trattamento** o **responsabili del trattamento** oppure **entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento** e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, **ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno,** al fine di garantire il risarcimento effettivo dell'interessato.*

*5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, **tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno** conformemente alle condizioni di cui al paragrafo 2.*

IMPORTANZA DEI CONTRATTI

DIRITTO AL RISARCIMENTO DEL DANNO

POSSIBILE AUMENTO DEL CONTENZIOSO

motivazioni

SANZIONI DI NATURA AMMINISTRATIVA

ART. 58 COMMA 2

Ogni autorità di controllo ha tutti i poteri correttivi seguenti:

*a) **rivolgere avvertimenti** al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;*

*b) **rivolgere ammonimenti** al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;*

*c) **ingiungere** al titolare del trattamento o al responsabile del trattamento **di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;***

***d) Ingiungere** al titolare del trattamento o al responsabile del trattamento **di conformare i trattamenti alle disposizioni del presente regolamento**, se del caso, in una determinata maniera ed entro un determinato termine;*

SANZIONI DI NATURA AMMINISTRATIVA

*e) ingiungere al titolare del trattamento di c**omunicare all'interessato una violazione dei dati personali;***

*f) imporre una l**imitazione provvisoria o definitiva al trattamento**, incluso il divieto di trattamento;*

*g) ordinare l**a rettifica, la cancellazione di dati personali o la limitazione del trattamento a** norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;*

***h) revocare la certificazione** o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;*

***i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure**, in funzione delle circostanze di ogni singolo caso; e*

j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

SANZIONE AMMNINISTRATIVA PECUNIARIA (art.83)

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte siano **in ogni singolo caso effettive, proporzionate e dissuasive**

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria ……si tiene debito conto dei seguenti elementi:

- **la natura, la gravità e la durata della violazione**
- **il carattere doloso o colposo della violazione;**
- **le misure adottate dal titolare del trattamento;**
- **il grado di responsabilità del titolare del trattamento**
- **eventuali precedenti**
- **il grado di cooperazione con l'autorità di**
- **le categorie di dati personali interessate dalla violazione;**
- **l'adesione ai codici di condotta**
- **eventuali altri fattori aggravanti o attenuanti**

SANZIONE STABILITA IN BASE AL FATTURATO PER LE AZIENDE

SANZIONI FINO A 10 MILIONI DI EURO
SANZIONI FINO A 20 MILIONI DI EURO

**SANZIONI AMMINISTRATIVE PECUNIARIE FINO A 10.000.000 €
O PER LE IMPRESE, FINO AL 2 % DEL FATTURATO MONDIALE**

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

SANZIONE AMMINISTRATIVA PECUNIARIA FINO A 20.0000 EURO

PER LE IMPRESE FINO AL 4% DEL FATTURATO MONDIALE

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

in Italia la disciplina per l'applicazione delle sanzioni amministrative pecuniarie è la

legge 689 del 1981

POSSIBILE EMANAZIONE DI LINEE GUIDA COMUNITARIE

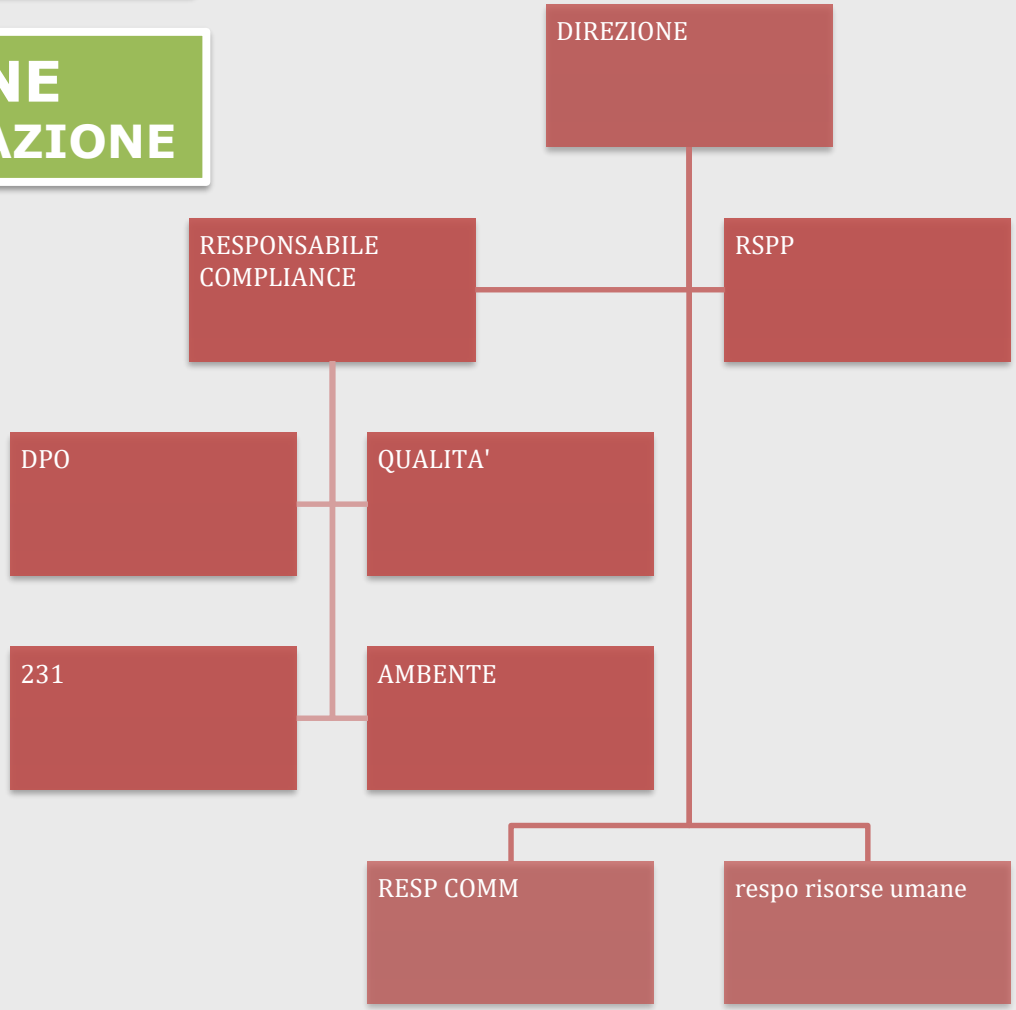
Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro ***può*** *prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.*

COME DIFENDERSI?

PREDISPONENDO LE PROVE

DEFINIRE L'ORGANIGRAMMA
DA CUI DERIVANO LE RESPONSABILITA'

FORMARE LE PERSONE
DARE EVIDENZA DELLA FORMAZIONE



CURARE ED AGGIORNARE

LA DOCUMENTAZIONE

ED

I CONTRATTI

EFFETTUARE L'ANALISI DEL RISCHIO

rischio	misure di mitagazione in essere	valore probabilità (quante volte è successo in passato)	valore gravità (quali sono le conseguenze)	valore rischio	misure di mitagazione e pianificazione
Carenza di consapevolezza (rischio di diffusione dei dati personali e sanitari)	incarichi dati agli operatori sanitari	Bassa	Alta (immagine dell'azienda)	media	implementare corsi di formazione per il personale sulla disciplina della privacy, sull'importanza degli aspetti privacy per la reputazione dell'azienda, sulle rilevanti sanzioni che possono colpire l'organizzazione
Azione di virus informatici o di codici malefici	antivirus sulla rete	bassa	alta	molto alta	**1)** sensibilizzare il personale circa i rischi esterni. 2)rivedere il regolamento interno del personale sull'accessibilitò al web. 3) aggiornare l'antivirus. 4) aumentare il numero di back up 5) rediere procedura interna per le situazioni in sui di verifica il virus
si sono riscontrati accessi non autorizzati ai locale del server ove conservati i dati dell'azienda	il server si trova in un locale chiuso a chiave	media	alta	alta	1) verificare chi ha le chiavi 2) valutare il cambio della serratura ed una gestione più corretta dei soggetti che possono accedere 3) 3) valutare la possibilità di accedere al locale solo tramitec odice accesso numerico o un sistema di impronte digitali

ART. 30 - REGISTRI DELLE ATTIVITA'

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati,

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

SEMPRE SE SI TRATTANO DATI SENSIBILI

VALUTAZIONE DEL RISCHIO

Art. 35
VALUTAZIONE DI IMPATTO
(sostituisce la notificazione)

quando serve:

uso di nuove tecnologie / trattamento dati sanitari su larga scala

cosa contiene

- **una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento,**
- **una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;**
- **una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;**
- **le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione**

GRAZIE
PER LA VOSTRA ATTENZIONE

www.studiolegalestefanelli.it
s.stefanelli@studiolegalestefanelli.it