UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CORSO DI PERFEZIONAMENTO IN
«SECURITY MANAGER»
CORSO DI FORMAZIONE IN
«PROFESSIONISTA DELLA SECURITY»

10 DICEMBRE 2021

FRANCESCO FARINA

SECURITY E PROFESSIONISTI DELLA SECURITY

1

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

STRUTTURAZIONE DELLA SECURITY IN AZIENDA

2

Classificazione di azienda

1_Scopo

1. **Imprese (aziende for profit):** realizzano utili per i soci o per l'imprenditore. Le imprese producono beni e/o servizi (output) per lo scambio, da cui derivano le entrate (ricavi) che vanno a remunerare i fattori produttivi (input) impiegati nel processo produttivo. L'obiettivo è la massimizzazione del valore del reddito d'esercizio
2. **Aziende pubbliche:** perseguono fini di interesse pubblico
3. **Aziende non profit:** perseguono fini sociali, assistenziali, culturali… Oltre che soddisfare i bisogni delle persone nel cui interesse sono costituite e gestite, è necessario che operino in condizioni di equilibrio economico, così come previsto per le imprese

3

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Classificazione di azienda

2_Natura del soggetto giuridico

Il soggetto giuridico è la persona o il gruppo di persone a cui fanno capo diritti e obblighi derivanti dall'attività compiuta in azienda. Distinguiamo in questo senso:

1. **Aziende private e non profit:** caratterizzate da un soggetto giuridico di tipo privato (Libro V c.c., Libro I c.c. e legislazioni speciali)
2. **Aziende pubbliche:** caratterizzate da un soggetto giuridico di natura pubblica, per cui soggette a norme di diritto amministrativo, Enti pubblici territoriali, Enti pubblici non economici ed economici, Organismi di diritto pubblico)

4

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Classificazione di azienda

2_Natura del soggetto giuridico

Enti pubblici non economici (Autonomia amministrativa ma non finanziaria, utilità sociale)

INPS, INAIL, UNIVERSITA', ENTI PARCO, ORDINI PROFESSIONALI, CROCE ROSSA, ACI

Enti pubblici economici (Autonomia amministrativa e finanziaria, utilità sociale)

AGENZIA DELLE ENTRATE, AGENZIA DEL DEMANIO

Organismi di diritto pubblico (Autonomia amministrativa e finanziaria, utilità sociale, concorrenti sul mercato)

ENAC, ENAV, IPAB,

5

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Classificazione di azienda

3_Forma giuridica

1. **Aziende individuali:** il soggetto giuridico è una persona fisica (il proprietario dell'azienda)
2. **Aziende collettive o società:** l'attività d'impresa è esercitata da due o più persone che svolgono in comune un'attività operativa, dietro l'apporto di capitali, al fine di dividere il rischio d'impresa. Il soggetto giuridico è quindi rappresentato da più persone fisiche o da una persona giuridica
   a) **Società di persone:** il soggetto giuridico è rappresentato dai singoli soci, titolari di diritti e obblighi derivanti dall'attività aziendale (Ss, Snc, Sas)
   b) **Società di capitali:** il soggetto giuridico è rappresentato dalla stessa società, che risulta titolare di diritti e obblighi (Spa, Sapa, Srl, Srls)

6

Classificazione di azienda

4_Settore di attività

1. **Aziende del settore primario:** svolgono attività di produzione originaria e utilizzano risorse disponibili in natura (agricole, ittiche, estrattive…)
2. **Aziende del settore secondario:** utilizzano e lavorano materiali forniti da altre aziende. Si caratterizzano per il ciclo di produzione (aziende artigiane, industriali)
3. **Aziende del settore terziario:** realizzano attività che hanno per oggetto la fornitura di servizi immateriali (aziende di trasporto, bancarie e assicurative, alberghiere…)

7

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Classificazione di azienda

5_Dimensioni

In dottrina…

- *Una grande impresa è quella in grado di esercitare un elevato grado di controllo del mercato, che cioè con le sue politiche riesce ad influenzare il comportamento delle altre imprese e a indirizzare la domanda dei consumatori o utilizzatori dei suoi prodotti*
- *Le piccole imprese sono quelle che non riescono a influenzare le variabili di mercato e che sono esposte, quindi, al mutamento sia della domanda che dell'offerta*
- *L'impresa di media dimensione, sotto il profilo dei rapporti con il mercato, risulta meglio assimilabile alla piccola impresa*

8

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Classificazione di azienda

5_Dimensioni

In pratica…

I 2 requisiti sono cumulativi, nel senso che devono sussistere entrambi

Dimensione impresa	Occupati	Fatturato (F)/Totale di Bilancio (TB) annui
MICRO	Inferiore a 10	F o TB non superiore a 2 milioni di €
PICCOLA	Da 10 a 49	F o TB non superiore a 10 milioni di €
MEDIA	Da 50 a 249	F non superiore a 50 milioni di € TB non superiore a 43 milioni di €
GRANDE	Oltre 249	F superiore a 50 milioni di € TB superiore a 43 milioni di €

PMI

DECRETO 18 aprile 2005 del Ministero delle Attività Produttive Adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese. (GU Serie Generale n.238 del 12-10-2005)

9

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Classificazione di azienda

6_Mercato

1. **Aziende che operano in un mercato concorrenziale:** è il caso delle imprese. Il mercato è concorrenziale sia dal lato della domanda (per l'acquisizione dei fattori produttivi) che dal lato dell'offerta (per il collocamento dei propri prodotti)
2. **Aziende che operano in un mercato non concorrenziale:** aziende che operano in mercati caratterizzati da una concorrenza «attenuata» o assente, dal lato della domanda o dal lato dell'offerta o in entrambi i casi. In questo senso, si distingue tra:
   a) **Aziende cooperative**
   b) **Amministrazioni pubbliche**
   c) **Aziende non profit**

10

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Classificazione di azienda

6_Mercato

a) **Aziende cooperative:** operano in un mercato parzialmente concorrenziale dal lato della domanda e/o dell'offerta in quanto i fornitori di alcuni fattori produttivi o i clienti coincidono con i proprietari dell'azienda stessa

b) **Amministrazioni pubbliche:** operano dal lato dell'offerta in mercati non concorrenziali in quanto cedono i propri servizi alla collettività dietro un corrispettivo che non corrisponde al prezzo di mercato e acquisiscono buona parte dei mezzi finanziari attraverso l'imposizione tributaria

c) **Aziende non profit:** operano dal lato della domanda e dell'offerta in un ambiente non concorrenziale. In molti casi acquisiscono i fattori produttivi gratuitamente o a valori non di mercato (donazioni, volontariato…) e cedono beni e servizi sempre gratuitamente o a valori non di mercato (servizi sociali, sanitari…)

11

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Classificazione di azienda

7_Localizzazione dei mercati di vendita

1. **Aziende locali:** si rivolgono ad un mercato locale (a livello comunale, provinciale o al massimo regionale)
2. **Aziende nazionali:** operano su tutto il mercato nazionale o su una parte rilevante di esso
3. **Aziende multinazionali:** il mercato a cui si rivolgono è globale (orizzontali, verticali, diversificate)

12

Classificazione di azienda

8_Livello di indipendenza

1. **Aziende Autonome:** non hanno rapporti societari con altre aziende o quando la partecipazione nel capitale di altra società (o la partecipazione di altra società nel suo capitale) è inferiore al 25% delle azioni (o diritto di voto)
2. **Aziende Partner:** la partecipazione azionaria è compresa tra il 25% e il 50%
3. **Aziende Collegate:** partecipazione nel capitale aziendale si spinge oltre il 50%, invece, secondo le raccomandazioni della Commissione europea, le due società possono definirsi collegate.

13

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le caratteristiche dell'organizzazione

- Un'organizzazione è caratterizzata da un gruppo di individui che svolgono attività interdipendenti, per il raggiungimento di obiettivi e che sviluppano e mantengono modelli di comportamento relativamente stabili e prevedibili, anche se gli individui dell'organizzazione possono cambiare
- 3 dimensioni che contribuiscono al formarsi dei modelli di comportamento organizzativo:
  - Complessità
  - Formalizzazione
  - Centralizzazione

14

Le caratteristiche dell'organizzazione

- Complessità: dipende dal numero di attività, di funzioni, di compiti, dal grado di eterogeneità e dal tipo di interdipendenza tra queste
- Grado di formalizzazione: si riferisce all'intensità di impiego di politiche, procedure, routine, regole formali e scritte, che vincolano le scelte dei membri dell'organizzazione
- Centralizzazione: fa riferimento alla distribuzione del potere e dell'autorità all'interno dell'organizzazione

15

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le caratteristiche dell'organizzazione

Le 3 dimensioni si riflettono nella struttura organizzativa e nella cultura organizzativa:

- Struttura organizzativa: fa riferimento alle relazioni tra i compiti svolti dai membri dell'organizzazione e si concretizza nelle forme di divisione del lavoro, nelle unità organizzative, nella gerarchia, nelle politiche, regole e procedure e nei diversi meccanismi di coordinamento e controllo
- Cultura organizzativa: è l'insieme dei valori dominanti, opinioni, atteggiamenti e norme che sono la base per giustificare decisioni e comportamenti

16

L'organizzazione e l'ambiente

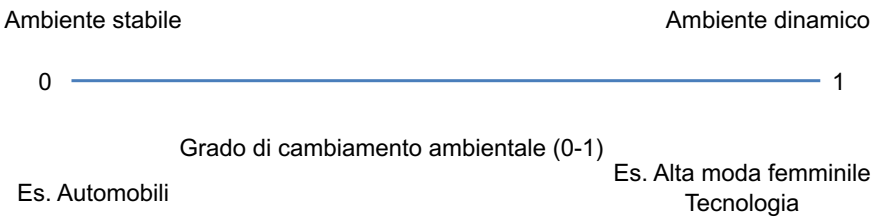
- L'insieme delle istituzioni, organizzazioni e attori al di fuori dell'organizzazione di riferimento, che forniscono input o che impiegano gli output dell'organizzazione è definito *ambiente rilevante (o transazionale)*
- L'ambiente rilevante include:
  - Mercati/clienti
  - Fornitori
  - Concorrenti
  - Sindacati
  - Gruppi di interesse
  - Leggi e normative
  - Investitori
  - Tecnologia

Stakeholders o ***«portatori di interesse»,*** che influenzano l'organizzazione

17

L'organizzazione e l'ambiente

- Il processo di adattamento delle organizzazioni all'ambiente è determinato dal grado di cambiamento ambientale e ciò ha un diretto impatto sulla struttura interna dell'organizzazione, sui processi, sulla cultura organizzativa in generale (a seconda della stabilità o del dinamismo ambientale)



18

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

L'organizzazione e l'ambiente

Organizzazione meccanica

- Efficienza: condizione essenziale per la sopravvivenza
- Mansioni molto ripetitive, routinarie e semplici
- Divisione del lavoro intensa
- Specializzazione elevata
- Compiti parcellizzati
- Attribuzioni di autorità e responsabilità molto chiare e formalizzate
- Struttura rigida e gerarchica
- Comunicazione verticale, top-down
- Poca autonomia decisionale ai livelli più bassi
- **Imprese che producono auto, acciaio, fast food**

19

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

L'organizzazione e l'ambiente

Organizzazione meccanica

- Il segreto del successo di McDonald's si basa su 4 fattori chiave:
- **Efficienza**: offre un metodo ottimale per passare, nel minor tempo possibile e con le migliori garanzie di sicurezza, da uno stato di appetito a quello del suo soddisfacimento
- **Calcolabilità**: enfasi sulla quantità più che sulla qualità (dimensioni della porzione, costo e tempo risparmiato rispetto al cucinarsi un pasto da sé)
- **Prevedibilità**: garanzia che i prodotti e i servizi offerti dall'impresa saranno gli stessi nel tempo e nello spazio (No surprises)
- **Controllo**: fila, limitatezza del menu, scarse possibilità di scelta
- https://www.youtube.com/watch?v=1DuYVuLgQ9U

G. Ritzer, sociologo americano, in «The McDonaldization of Society», 1993.

20

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

L'organizzazione e l'ambiente

Organizzazione organica

- Flessibilità
- Relazioni e compiti definiti in modo meno netto e preciso
- Mansioni più ampie
- Informazioni decentrate
- Comunicazione più orizzontale e meno verticale
- Processi decisionali orientati da poche e chiare linee guida
- Focus sulla competenza e non sulla posizione ricoperta
- Si lavora per progetti e per processi: no unica dipendenza gerarchica
- **Imprese di consulenza, pubblicità, R&S…**

21

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

L'organizzazione e l'ambiente

Organizzazione mista dominata tecnologicamente

- Doppia veste:
- Unità tecnologiche e di R&S sono di tipo organico e flessibili (maggiore autonomia decisionale e libertà d'azione)
- L'unità di marketing ha una struttura più burocratica, a causa del mercato maggiormente stabile (compiti, mansioni, ruoli e responsabilità più precisi, minor grado di decentramento decisionale)
- Ciò può comportare tensioni e conflitti interfunzionali
- **Imprese che producono e vendono pc, Compaq, Dell…**

22

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

L'organizzazione e l'ambiente

Organizzazione mista dominata dal mercato

- Doppia veste:
- Unità tecniche e di produzione con struttura relativamente rigida e gerarchica
- Le unità di marketing e di distribuzione più flessibili e con maggiore autonomia decisionale
- Come nella MDT, anche qui possono sorgere problemi nel coordinamento e nell'integrazione delle unità organizzative maggiormente organiche con quelle maggiormente meccaniche
- **Imprese operanti nei settori della musica, della produzione cinematografica e dell'alta moda**

23

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La progettazione organizzativa

Definizione

Progettare una struttura organizzativa vuol dire definire, per tutte le persone e per tutte le unità organizzative, le modalità con cui vengono suddivise e coordinate le singole attività lavorative

Obiettivo della progettazione è quello di definire i compiti, le responsabilità e i meccanismi di coordinamento al fine di orientare i comportamenti dei singoli e dei gruppi al perseguimento dei fini che l'organizzazione si è data

24

La progettazione organizzativa

Le unità organizzative sono create attraverso due processi sequenziali:

1. ***Differenziazione:*** processo di scomposizione di tutte le attività di lavoro dell'organizzazione e di separazione di specifici insiemi di attività da altri (sulla base dei prodotti/servizi, progetti, tecniche impiegate, localizzazione geografica, tipologia di clienti…)
2. ***Integrazione:*** processo di creazione del coordinamento, attraverso appropriati meccanismi strutturali e interpersonali, delle attività delle differenti unità organizzative (legami molto stretti e ben definiti o connessioni deboli)

25

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La progettazione organizzativa

DIVISIONE DEL LAVORO E INTERDIPENDENZE

Il caso

Supponiamo di essere un falegname talentuoso e di avviare la nostra impresa, Mobiletti s.n.c.

All'inizio ci occupiamo di tutto in prima persona: siamo a contatto con i clienti, acquistiamo i materiali, assembliamo, produciamo, consegniamo, installiamo…

Dopo qualche tempo registriamo un certo successo, ma ormai, con la clientela e le commesse che sono aumentate, non ce la facciamo più a gestire tutto da soli… e ci troviamo costretti a dover assumere qualcuno… ma come dividiamo il lavoro?!?

26

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La progettazione organizzativa

DIVISIONE DEL LAVORO E INTERDIPENDENZE

Il caso

Task specialization VS personal specialization (in base al livello di conoscenze/abilità richiesto)

Quando i compiti sono divisi e quando compiti distinti, eseguiti da persone diverse, sono necessari per completare un progetto, un prodotto, un servizio, o un semilavorato, si viene a creare un'*interdipendenza* tra i compiti.

Esistono 3 tipi di interdipendenza:

- SEQUENZIALE
- RECIPROCA
- GENERICA

Il concetto di interdipendenza è applicabile a varie unità di analisi: ai compiti, alle persone, alle attività, alle unità organizzative, alle organizzazioni…

27

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La progettazione organizzativa

SEQUENZIALE

DIVISIONE DEL LAVORO E INTERDIPENDENZE

Il caso

In termini di relazione input-output possiamo affermare che esiste interdipendenza sequenziale quando l'output di A rappresenta un input per B, l'output di B rappresenta un input per C e così via

28

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La progettazione organizzativa

RECIPROCA

DIVISIONE DEL LAVORO E INTERDIPENDENZE

Il caso

Quando i compiti svolti da 2 o più persone sono vicendevolmente dipendenti in termini input-output, allora l'interdipendenza è reciproca: il falegname e lo specialista dipendono l'uno dall'altro per completare il lavoro con successo

29

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

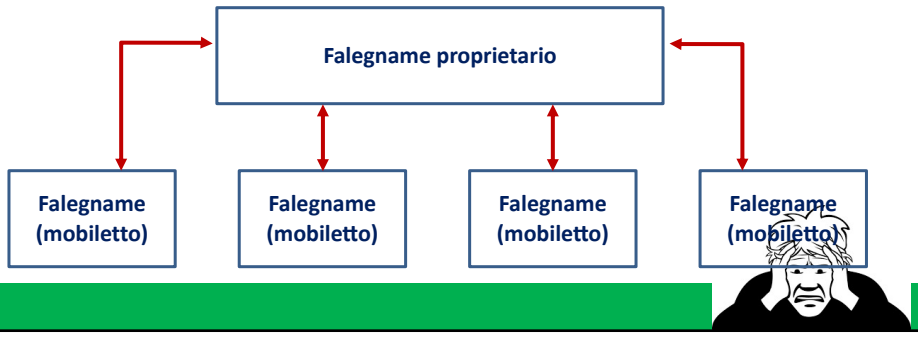
La progettazione organizzativa

GENERICA

DIVISIONE DEL LAVORO E INTERDIPENDENZE

Il caso

Nell'interdipendenza generica viene a mancare il rapporto input-output; si lavora in modo più autonomo e i compiti e le attività svolte non dipendono direttamente dal lavoro di altri



30

Le principali forme/strutture organizzative

In sintesi, una struttura organizzativa:

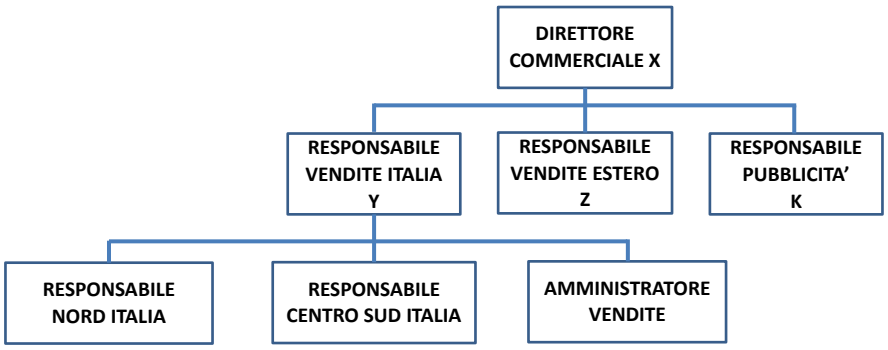
- indica i *rapporti di dipendenza formale*, compresi il numero di livelli gerarchici e l'ampiezza di controllo di manager e supervisori
- identifica il *raggruppamento di individui* in unità organizzative
- implica la progettazione di *sistemi* che assicurino una *comunicazione* e un *coordinamento* efficaci

La rappresentazione visiva di questi elementi è rappresentata dall'**organigramma aziendale**

31

Le principali forme/strutture organizzative

ORGANIGRAMMA



L'organigramma aziendale è una rappresentazione formale del sistema organizzativo aziendale, definisce l'articolazione degli organi (compresi staff e line) e descrive le relazioni gerarchiche tra di essi

32

Le principali forme/strutture organizzative

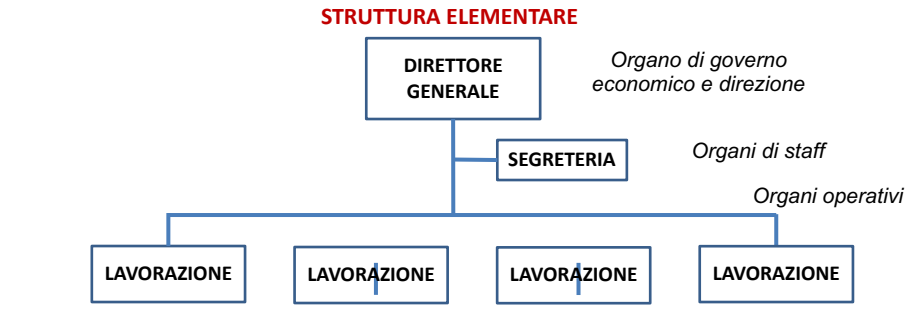
Tre principali tipologie di struttura:

- ***Elementare***: adatta ad imprese di piccole dimensioni, con combinazioni produttive semplici, un solo prodotto o una linea di prodotti molto omogenea, destinata ad un solo mercato
- ***Funzionale***: principale assetto organizzativo delle imprese di medie dimensioni, con un solo prodotto o linea di prodotti omogenea, destinata ad un solo mercato
- ***Divisionale***: adatta ad imprese di medio/grandi dimensioni e combinazioni produttive complesse, diversi prodotti o linee di prodotti disomogenee, destinati a specifici e diversi mercati

33

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le principali forme/strutture organizzative

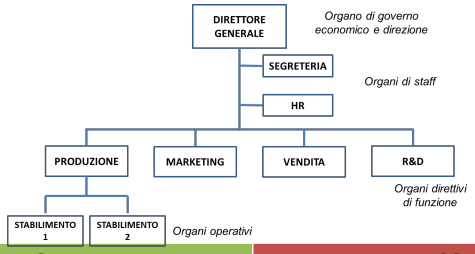


PRO → → →	CONTRO
Elevata flessibilità di breve periodo	Limite alla crescita nel lungo periodo
Processo decisionale accentrato	Problemi concentrati al vertice
Bassi costi di struttura	Sbilanciamento operativo
Rapporti interpersonali costanti	

34

Le principali forme/strutture organizzative

STRUTTURA FUNZIONALE



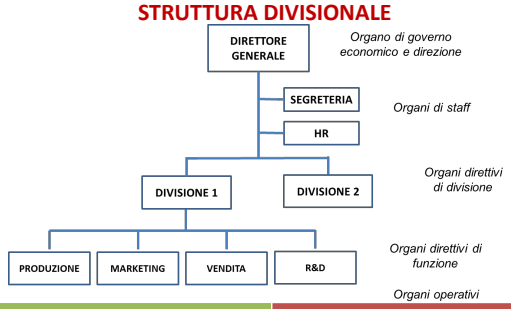
PRO	CONTRO
Elevato accentramento con partecipazione degli organi direttivi di funzione	Sorgere di conflitti interfunzionali
Economie di apprendimento (raggruppamento in base alle competenze)	Sovraccarico di informazioni al vertice (gestione e monitoraggio)
Economie di scala	Scarsa capacità di gestire un portafoglio prodotti più ricco
Rapporti interpersonali costanti	Non adatta a differenziazione di prodotto o geografica

35

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le principali forme/strutture organizzative

STRUTTURA DIVISIONALE



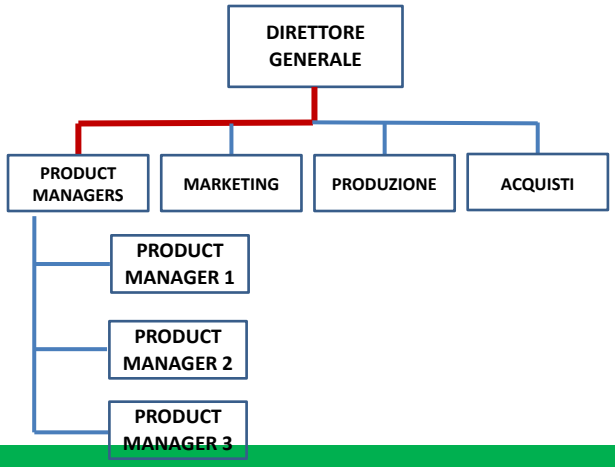
PRO	CONTRO
Diffusa autonomia decisionale-organizzativa	Eccesso di decentramento organizzativo
Elevata capacità di gestire un portafoglio prodotti ricco e in diverse sedi	Costi elevati a causa della duplicazione di funzioni (diseconomie di scala)
Possibilità di pianificazione a lungo termine da parte del vertice	Competizione tra le divisioni per accaparrarsi le risorse → mancanza di cooperazione → peggioramento della performance dell'organizzazione
Possibilità per i responsabili di divisione di sviluppare specifiche capacità imprenditoriali	

36

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le principali forme/strutture organizzative

LA STRUTTURA FUNZIONALE MODIFICATA PER PRODOTTO_1

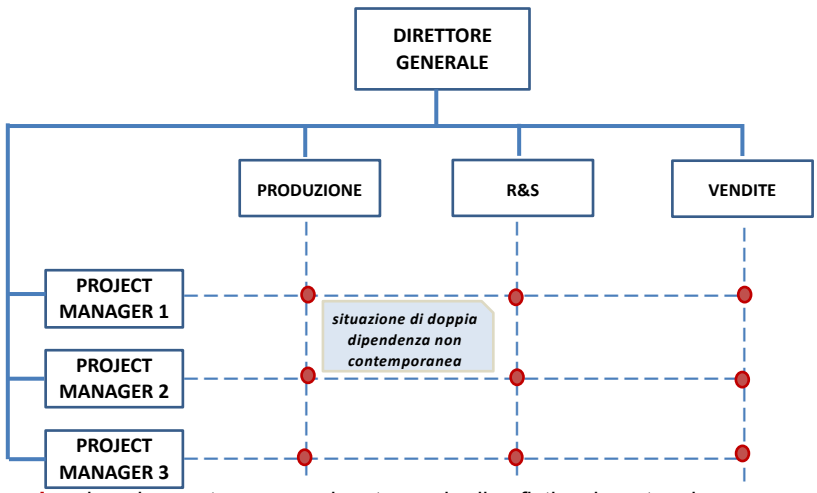


37

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le principali forme/strutture organizzative

LA STRUTTURA FUNZIONALE MODIFICATA PER PROGETTO



Quando: si vuole mantenere un elevato grado di sofisticazione tecnica e, contemporaneamente, è necessario raggiungere uno specifico obiettivo, rappresentato da un progetto

38

Le principali forme/strutture organizzative

LA STRUTTURA PER PROCESSI

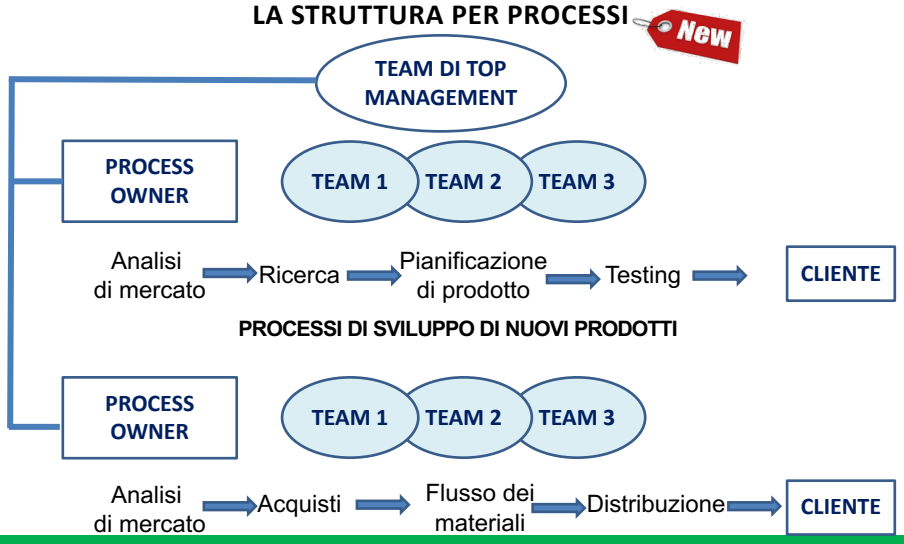
- **Quando:** il contesto è caratterizzato dalla flessibilità, dalla velocità e dal cambiamento organizzativo
- Nata a seguito dei cambiamenti intervenuti negli ultimi anni
- La divisione del lavoro e il criterio di specializzazione della struttura è per processi chiave interfunzionali
- I responsabili dei processi, che attraversano tutta l'organizzazione e coinvolgono diversi specialisti, sono chiamati process owner, e hanno la responsabilità di tutto il processo e dei team coinvolti
- Ogni team è relativamente autonomo nelle decisioni, tranne quelli interdipendenti
- L'obiettivo principale è la generazione del valore per il cliente

39

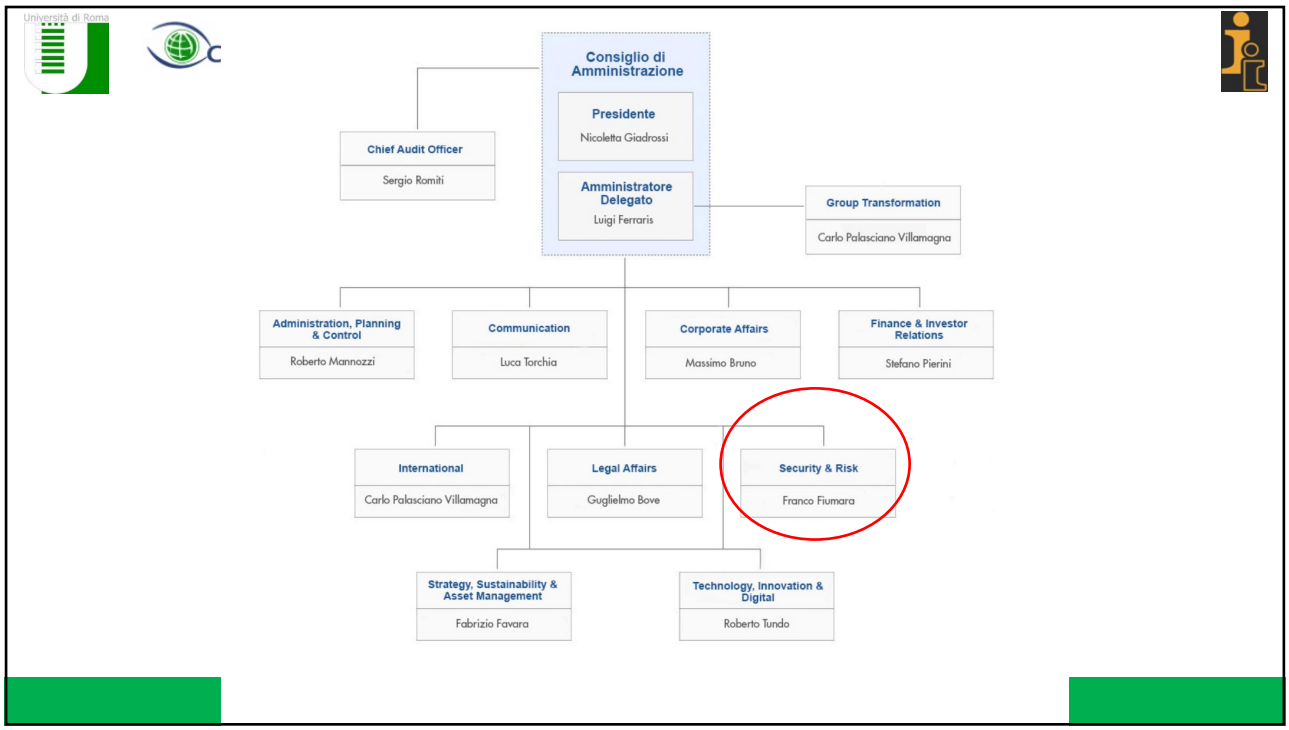
UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le principali forme/strutture organizzative

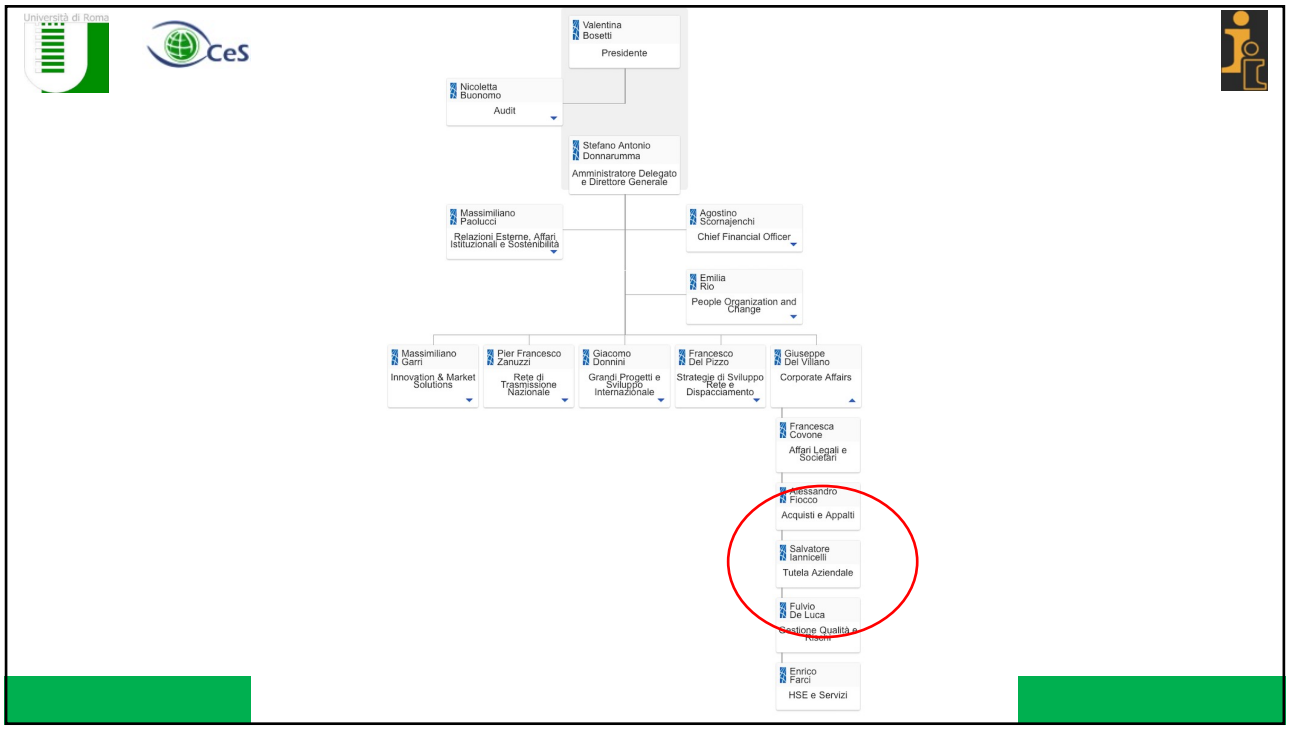
LA STRUTTURA PER PROCESSI



40


Consiglio di Amministrazione
Presidente
Nicoletta Giadrossi
Amministratore Delegato
Luigi Ferraris
Chief Audit Officer
Sergio Romiti
Group Transformation
Carlo Palasciano Villamagna
Administration, Planning & Control
Roberto Mannozzi
Communication
Luca Torchia
Corporate Affairs
Massimo Bruno
Finance & Investor Relations
Stefano Pierini
International
Carlo Palasciano Villamagna
Legal Affairs
Guglielmo Bove
Security & Risk
Franco Fiumara
Strategy, Sustainability & Asset Management
Fabrizio Favara
Technology, Innovation & Digital
Roberto Tundo

41


Valentina Bosetti
Presidente
Nicoletta Buonomo
Audit
Stefano Antonio Donnarumma
Amministratore Delegato e Direttore Generale
Massimiliano Paolucci
Relazioni Esterne, Affari Istituzionali e Sostenibilità
Agostino Scornajenchi
Chief Financial Officer
Emilia Rio
People Organization and Change
Massimiliano Garri
Innovation & Market Solutions
Pier Francesco Zanuzzi
Rete di Trasmissione Nazionale
Giacomo Donnini
Grandi Progetti e Sviluppo Internazionale
Francesco Del Pizzo
Strategie di Sviluppo Rete e Dispacciamento
Giuseppe Del Villano
Corporate Affairs
Francesca Covone
Affari Legali e Societari
Alessandro Fiocco
Acquisti e Appalti
Salvatore Iannicelli
Tutela Aziendale
Fulvio De Luca
Gestione Qualità e Rischi
Enrico Farci
HSE e Servizi

42

- https://www.eni.com/it-IT/investitori/risk-management.html

43

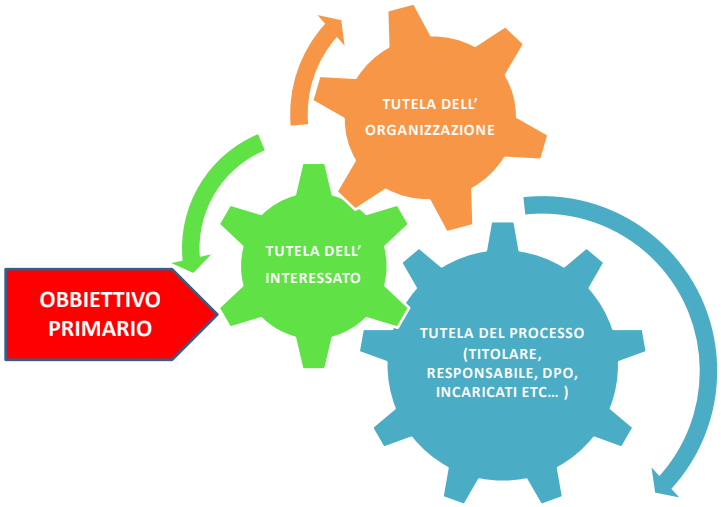
UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

STRUTTURAZIONE DI UN SISTEMA DI GESTIONE E PROTEZIONE DEI DATI PERSONALI IN AZIENDA

44

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

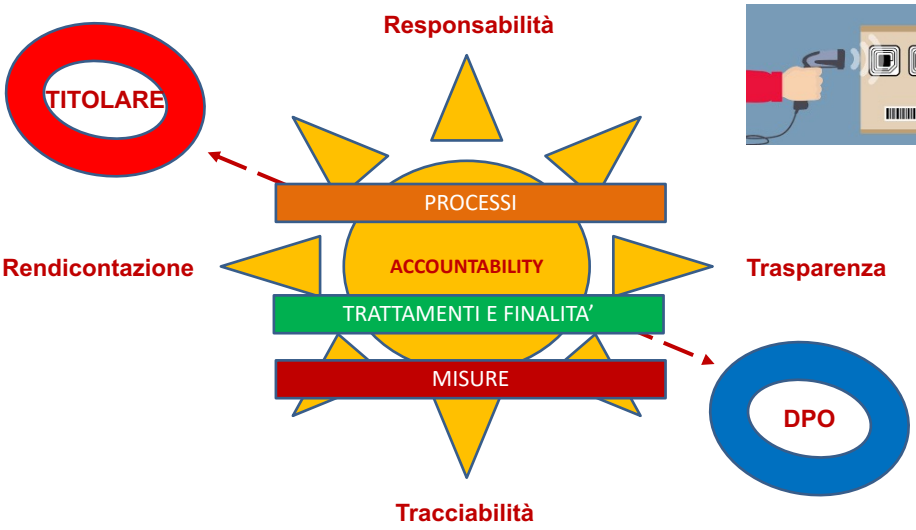
DATA PROTECTION E SECURITY



45

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

GDPR: RISK & ACCOUNTABILITY APROACH



46

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

GDPR: RISK & ACCOUNTABILITY APROACH

Titolare

Devono mettere in atto comportamenti proattivi a dimostrazione della concreta adozione di misure finalizzate ad assicurare l´applicazione del regolamento (23-25)

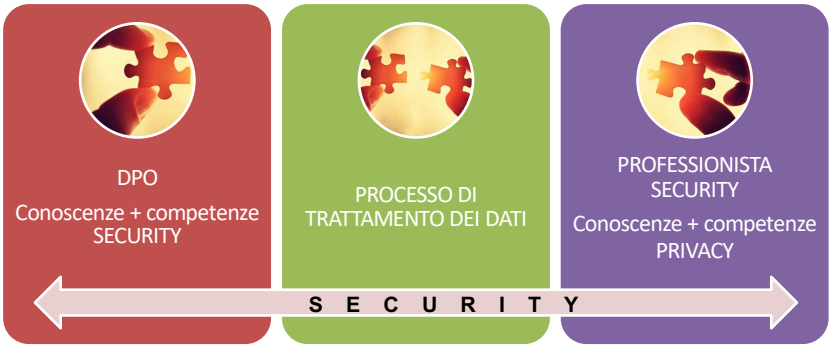
Responsabile Protezione Dati (DPO)

DATA PROTECTION «by default» and «by design» → **Prevedere da subito garanzie indispensabili per la tutela dei diritti degli interessati adatto al contesto in cui si colloca il trattamento (25)** → **Attività specifiche e dimostrabili per dimostrare di essere in grado di effettuare il trattamento**

47

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY



48

IL DATO PERSONALE

«GARANTE PRIVACY»:

- Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..;

49

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

TIPOLOGIE DI DATI

DATI CHE CONSENTONO IDENTIFICAZIONE DELL'INTERESSATO DIRETTA O INDIRETTA

- nome e cognome - volto, impronte digitali o calligrafia - indirizzo email - numero di patente - numero identificativo nazionale - numero di passaporto- indirizzo IP - indirizzo di casa- numero di targa del veicolo - numeri di carta di credito - identità digitale - data di nascita - luogo di nascita - informazioni genetiche - numero di telefono - account name o nickname -

DATI PARTICOLARI

- origine razziale o etnica - convinzioni religiose o filosofiche - opinioni politiche - appartenenza sindacale – dati sanitari - dati relativi alla alla vita o all'orientamento sessuale - i dati genetici - dati biometrici;

geolocalizzazione

DATI GIUDIZIARI

relativi a condanne penali

provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale - provvedimenti penali di condanna definitivi - Libertà condizionale - divieto od obbligo di soggiorno.

50

LA NORMATIVA IN ESSERE

51

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DISCIPLINA ATTUALE

La materia è regolamentata da

- Il Regolamento generale per la protezione dei dati personali 2016/679 (General Data Protection Regulation o GDPR) – la principale normativa europea in materia di protezione dei dati personali. Il Regolamento generale per la protezione dei dati personali 2016/679 (General Data Protection Regulation o GDPR (entrato in vigore il 25 Maggio 2018)
- D. lgs n. 196/2003 o codice della Privacy o "Codice in materia di protezione dei dati personali",
- D. lgs n. 101/2018 che ha recepito il GDPR nella normativa italiana e modificato il D.lgs 196. (Emanato a Dicembre 2018)
- Il regolamento era immediatamente applicabile, ed il recepimento e le modifiche fatte al 196 lo rendono ancora attuale.

52

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL REGOLAMENTO

CAPO I - Disposizioni generali
Articolo 1 - Oggetto e finalità
Articolo 2 - Ambito di applicazione materiale
Articolo 3 - Ambito di applicazione territoriale
Articolo 4 - Definizioni

CAPO II - Principi
Articolo 5 - Principi applicabili al trattamento di dati personali
Articolo 6 - Liceità del trattamento
Articolo 7 - Condizioni per il consenso
Articolo 8 - Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione
Articolo 9 - Trattamento di categorie particolari di dati personali
Articolo 10 - Trattamento dei dati personali relativi a condanne penali e reati
Articolo 11 - Trattamento che non richiede l'identificazione

CAPO III - Diritti dell'interessato
Sezione 1 - Trasparenza e modalità
Articolo 12 - Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato
Sezione 2 - Informazione e accesso ai dati personali
Articolo 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato
Articolo 14 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato
Articolo 15 - Diritto di accesso dell'interessato
Sezione 3 - Rettifica e cancellazione
Articolo 16 - Diritto di rettifica
Articolo 17 - Diritto alla cancellazione («diritto all'oblio»)
Articolo 18 - Diritto di limitazione di trattamento
Articolo 19 -Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento
Articolo 20 - Diritto alla portabilità dei dati
Sezione 4 - Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche
Articolo 21 - Diritto di opposizione
Articolo 22 - Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione
Sezione 5 – Limitazioni
Articolo 23 - Limitazioni

53

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL REGOLAMENTO

CAPO IV - Titolare del trattamento e responsabile del trattamento
Sezione 1 - Obblighi generali
Articolo 24 - Responsabilità del titolare del trattamento
Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
Articolo 26 - Contitolari del trattamento
Articolo 27 - Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione
Articolo 28 - Responsabile del trattamento
Articolo 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento
Articolo 30 - Registri delle attività di trattamento
Articolo 31 - Cooperazione con l'autorità di controllo
Sezione 2 - Sicurezza dei dati personali
Articolo 32 - Sicurezza del trattamento
Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo
Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato
Sezione 3 - Valutazione d'impatto sulla protezione dei dati e consultazione preventiva
Articolo 35 - Valutazione d'impatto sulla protezione dei dati
Articolo 36 - Consultazione preventiva
Sezione 4 - Responsabile della protezione dei dati
Articolo 37 - Designazione del responsabile della protezione dei dati
Articolo 38 - Posizione del responsabile della protezione dei dati
Articolo 39 - Compiti del responsabile della protezione dei dati
Sezione 5 - Codici di condotta e certificazione
Articolo 40 - Codici di condotta
Articolo 41 - Monitoraggio dei codici di condotta approvati
Articolo 42 - Certificazione
Articolo 43 - Organismi di certificazione

CAPO V - Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
Articolo 44 - Principio generale per il trasferimento
Articolo 45 - Trasferimento sulla base di una decisione di adeguatezza
Articolo 46 - Trasferimento soggetto a garanzie adeguate
Articolo 47 - Norme vincolanti d'impresa
Articolo 48 - Trasferimento o comunicazione non autorizzati dal diritto dell'Unione
Articolo 49 - Deroghe in specifiche situazioni
Articolo 50 - Cooperazione internazionale per la protezione dei dati personali

CAPO VI - Autorità di controllo indipendenti
Sezione 1 – Indipendenza
Articolo 51 - Autorità di controllo
Articolo 52 – Indipendenza
Articolo 53 - Condizioni generali per i membri dell'autorità di controllo
Articolo 54 - Norme sull'istituzione dell'autorità di controllo
Sezione 2 - Competenza, compiti e poteri
Articolo 55 - Competenza
Articolo 56 - Competenza dell'autorità di controllo capofila
Articolo 57 - Compiti
Articolo 58 - Poteri
Articolo 59 - Relazioni di attività

CAPO VII - Cooperazione e coerenza
Sezione 1 - Cooperazione
Articolo 60 - Cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate
Articolo 61 - Assistenza reciproca
Articolo 62 - Operazioni congiunte delle autorità di controllo
Sezione 2 - Coerenza
Articolo 63 - Meccanismo di coerenza
Articolo 64 - Parere del comitato europeo per la protezione dei dati
Articolo 65 - Composizione delle controversie da parte del comitato
Articolo 66 - Procedura d'urgenza
Articolo 67 - Scambio di informazioni
Sezione 3 - Comitato europeo per la protezione dei dati
Articolo 68 - Comitato europeo per la protezione dei dati
Articolo 69 - Indipendenza
Articolo 70 - Compiti del comitato
Articolo 71 - Relazioni
Articolo 72 - Procedura
Articolo 73 - Presidente
Articolo 74 - Compiti del presidente
Articolo 75 - Segreteria
Articolo 76 - Riservatezza

54

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL REGOLAMENTO

CAPO VIII - Mezzi di ricorso, responsabilità e sanzioni
Articolo 77 - Diritto di proporre reclamo all'autorità di controllo
Articolo 78 - Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo
Articolo 79 - Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento
Articolo 80 - Rappresentanza degli interessati
Articolo 81 - Sospensione delle azioni
Articolo 82 - Diritto al risarcimento e responsabilità
Articolo 83 - Condizioni generali per infliggere sanzioni amministrative pecuniarie
Articolo 84 - Sanzioni

CAPO IX - Disposizioni relative a specifiche situazioni di trattamento
Articolo 85 - Trattamento e libertà d'espressione e di informazione
Articolo 86 - Trattamento e accesso del pubblico ai documenti ufficiali
Articolo 87 -Trattamento del numero di identificazione nazionale
Articolo 88 - Trattamento dei dati nell'ambito dei rapporti di lavoro
Articolo 89 - Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
Articolo 90 - Obblighi di segretezza
Articolo 91 - Norme di protezione dei dati vigenti presso chiese e associazioni religiose

CAPO X - Atti delegati e atti di esecuzione
Articolo 92 - Esercizio della delega
Articolo 93 - Procedura di comitato

CAPO XI - Disposizioni finali
Articolo 94 - Abrogazione della direttiva 95/46/CE
Articolo 95 - Rapporto con la direttiva 2002/58/CE
Articolo 96 - Rapporto con accordi precedentemente conclusi
Articolo 97 - Relazioni della Commissione
Articolo 98 - Riesame di altri atti legislativi dell'Unione in materia di protezione dei dati
Articolo 99 - Entrata in vigore e applicazione

55

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CAPO 1 - DISPOSIZIONI GENERALI

DA ART. 1 (OGGETTO E FINALITA')

- **.....protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali**

DA ART. 2 (AMBITI DI APPLICAZIONE MATERIALE)

- **.....si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi**
- **.....non si applica ai trattamenti di dati personali:**
  - **effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico**
  - **effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse**

56

CAPO 1 - DISPOSIZIONI GENERALI

DA ART. 3 (AMBITO DI APPLICAZIONE TERRITORIALE)

- **……si applica al trattamento dei dati personali da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.**
- **……si applica al trattamento dei dati personali di interessati dell'Unione, anche se effettuato da un titolare o responsabile non stabilito nell'Unione, quando le attività di trattamento riguardano:**
  - **a) l'offerta di beni o la prestazione di servizi a interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;**
  - **b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.**

57

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CAPO 1 - DISPOSIZIONI GENERALI

DA ART. 4 (DEFINIZIONI)

- **……si applica al trattamento dei dati personali da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.**

58

I PRINCIPI FONDANTI DELLA NUOVA PRIVACY

59

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CAPO 2 - PRINCIPI

DA ART. 5 (PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI)

- **….. Liceità, correttezza e trasparenza**
- **….. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità**
- **….. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»)**
- **….. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);**

60

CAPO 2 - PRINCIPI

DA ART. 5 (PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI)

- **…… conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; (periodi più lunghi per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, Art. 89, paragrafo 1, con misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);**
- **…… trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).**

61

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CAPO 2 - PRINCIPI

DA ART. 6 (LA LICEITA')

- **…… Il trattamento è considerabile lecito solo se:**
  - **a) l'interessato ha espresso il consenso;**
  - **b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte….;**
  - **c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare**
  - **d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica**
  - **e) Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;**
  - **f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.**

62

CAPO 2 - PRINCIPI

QUANDO SUSSISTE IL LEGITTIMO INTERESSE

- misure di sicurezza;
- trasferimento di dati tra parti diverse della stessa azienda;
- elaborazione al fine di verifica dell'età;
- valutazione del rischio;
- esercizio del diritto di opposizione (vedi paragrafo successivo) ad esempio nel marketing diretto, nel qual caso può essere necessario mantenere la mail per impedire l'invio di ulteriori comunicazione commerciali;
- personalizzazione del sito web per migliorare l'esperienza dell'utente;
- analisi web, verifica del numero di visitatori del sito, commenti, ecc...;
- comunicazione di reati all'autorità giudiziaria;
- in ambito lavorativo l'utilizzo di dati di localizzazione (smartphone, GPS);
- misure per la sicurezza delle reti e delle comunicazioni.

63

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CAPO 2 - PRINCIPI

***DA ART. 6 (LA BASE GIURIDICA PER GIUSTIFICARE IL TRATTAMENTO PER OBBLIGO LEGALE O INTERESSE PUBBLICO…*)**

- **…….cui al paragrafo 1, lettere c) ed e), deve essere stabilita:**
  a) **dal diritto dell'Unione;**
  b) **dal diritto dello Stato membro cui è soggetto il titolare.**

  Lo Stato membro può prevedere condizioni generali relative alla liceità del trattamento; alle tipologie di dati oggetto del trattamento; agli interessati; ai soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento…..

64

CAPO 2 - PRINCIPI

DA ART. 7 (LE CONDIZIONI PER IL CONSENSO…)

1. **Se il trattamento è basato sul consenso, il titolare deve essere in grado di dimostrare che l'interessato ha lo ha effettivamente prestato.**
2. **Se la richiesta di consenso è «inserita» in mezzo ad altri aspetti di una dichiarazione/documento deve essere chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.**
3. **L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. Deve essere informato della possibilità. Il trattamento è lecito fino al momento della revoca**
4. **Il consenso deve essere liberamente prestato, pertanto bisogna stare attenti che l'esecuzione di un contratto non sia vincolata alla prestazione del consenso**

65

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CAPO 2 - PRINCIPI

DA ART. 8 (IL CONSENSO DEI MINORI…)

1. **Qualora il consenso per «offerta diretta di servizi della società dell'informazione» sia prestato da un minore (articolo 6, paragrafo 1, lettera a), il trattamento di dati personali è lecito se il minore ha almeno 16 anni, se ha età inferiore a 16 anni, il trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.**
2. **Gli Stati membri possono stabilire per legge un' età inferiore purché non inferiore ai 13 anni.**
3. **Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili. (TIK TOK/YOU TUBE)**

66

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CAPO 2 - PRINCIPI

DA ART. 9 (LE CATEGORIE PARTICOLARI DI DATI PERSONALI…)

1. È vietato trattare categorie particolari di dati personali

2. a meno che:

a) l'interessato ha prestato il proprio consenso esplicito;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell' incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

67

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CAPO 2 - PRINCIPI

DA ART. 9 (LE CATEGORIE PARTICOLARI DI DATI PERSONALI…)

2. ……. a meno che:

e) riguarda dati personali resi manifestamente pubblici dall'interessato;

f) è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

g) il trattamento è necessario per motivi di interesse pubblico

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al para- grafo 3;

i) è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (articolo 89, paragrafo 1), sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. …… possono essere trattati per le finalità di cui alla lettera h), se sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto ……o da altra persona anch'essa soggetta all'obbligo di segretezza

68

I DIRITTI DELL'INTERESSATO

69

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

***DA ART. 12 (TRASPARENZA E MODALITA'…*)**

1. **Il titolare adotta misure appropriate per fornire all'interessato tutte le informazioni (art. 13 e 14, e le comunicazioni art. da 15 a 22 e 34) in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni desti- nate specificamente ai minori. …. per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.**
2. **Il titolare agevola l'esercizio dei diritti dell'interessato (arti 15 – 22). non può rifiutare di soddisfare la richiesta dell'interessato salvo dimostri che non è in grado di identificare l'interessato.**
3. **Il titolare del trattamento da riscontro all'interessato al più tardi entro un mese dal ricevimento della richiesta. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.**

70

DA ART. 12 (TRASPARENZA E MODALITA'…)

4. **Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.**

5) **Le informazioni sono gratuite, ma se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare può:**

- **a) addebitare un contributo spese ragionevole (per costi amministrativi sostenuti);**
- **b) rifiutare di soddisfare la richiesta (con onere di dimostrarne il carattere manifestamente infondato o eccessivo).**

6) **qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.**

71

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DA ART. 13 (LE INFORMAZIONI DA FORNIRE…); DA ART. 14

(PER DATI RACCOLTI PRESSO INTERESSATO)		*(PER DATI NON RACCOLTI PRESSO INTERESSATO)*	
a)	l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;	a)	l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b)	i dati di contatto del responsabile della protezione dei dati;	b)	i dati di contatto del responsabile della protezione dei dati;
c)	finalità e base giuridica del trattamento;	c)	finalità e base giuridica del trattamento;
d)	eventuali legittimi interessi perseguiti;	d)	le categorie di dati personali in questione;
e)	eventuali destinatari o categorie di destinatari dei dati personali;	e)	eventuali destinatari o categorie di destinatari dei dati personali;
f)	Eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e garanzie.	f)	Eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e garanzie.

72

DA ART. 13 (LE INFORMAZIONI DA FORNIRE…); DA ART. 14

(PER DATI RACCOLTI PRESSO INTERESSATO)		*(PER DATI NON RACCOLTI PRESSO INTERESSATO)*	
2)	**In aggiunta, nel momento in cui i dati personali sono ottenuti, fornisce ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:**	**2)**	**In aggiunta, nel momento in cui i dati personali sono ottenuti, fornisce ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:**
a)	**il periodo di conservazione o, i criteri utilizzati per determinarlo;**	**a)**	**il periodo di conservazione o, i criteri utilizzati per determinarlo;**
b)	**diritto di accesso, rettifica, cancellazione, limitazione che lo riguardano o di opposizione al loro trattamento, e portabilità dei dati;**	**b)**	**eventuali legittimi interessi perseguiti; (art.6 par.1)**
c)	**Diritto di revocarlo se trattamento basato su consenso (art. 6, paragrafo 1, lettera a; art. 9, paragrafo 2, lettera a), senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;**	**c)**	**diritto di accesso, rettifica, cancellazione, limitazione che lo riguardano o di opposizione al loro trattamento, e portabilità dei dati;**
d)	**diritto di proporre reclamo a un'autorità di controllo;**	**d)**	**Diritto di revocarlo se trattamento basato su consenso (art. 6, paragrafo 1, lettera a; art. 9, paragrafo 2, lettera a), senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;**

73

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DA ART. 15 (DIRITTO DI ACCESSO…)

1. L'interessato ha il diritto di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) finalità del trattamento;
b) categorie di dati personali in questione;
c) destinatari o le categorie di destinatari a cui sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) il periodo di conservazione dei dati personali, i criteri utilizzati per determinarlo;
e) Sul diritto di chiedere al titolare del trattamento esercizio degli altri diritti;
f) Sul diritto di proporre reclamo a un' autorità di controllo;
g) sull'origine dei dati se non raccolti da interessato;
h) Eventuale processo decisionale automatizzato, compresa la profilazione
i) Garanzie in caso di trasferimento a paesi terzi

74

DA ART. 16 (DIRITTO DI RETTIFICA…)

L'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti o incompleti che lo riguardano senza ingiustificato ritardo.

DA ART. 17 (DIRITTO DI CANCELLAZIONE…)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei propri dati personali senza ingiustificato ritardo se sussiste uno dei motivi seguenti:

a) **i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;**
b) **l'interessato revoca il consenso;**
c) **l'interessato si oppone al trattamento e non esistono i presupposti per poterlo fare ;**
d) **i dati personali sono stati trattati illecitamente;**
e) **i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro;**
f) **i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ('articolo 8, paragrafo 1 – minori)**

se i dati personali sono stati resi pubblici e si è obbligati a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione si devono adottare misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

75

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DA ART. 18 (DIRITTO DI LIMITAZIONE AL TRATTAMENTO…)

diritto di ottenere la limitazione quando:

a) **l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;**
b) **il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;**
c) **benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;**
d) **l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.**

DA ART. 19 (DIRITTO DI NOTIFICA…)

Il titolare del trattamento comunica a TUTTI i destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

76

DA ART. 20 (DIRITTO ALLA PORTABILITA'…)

1. **L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:**
   a) **il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o del- l'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e**
   b) **il trattamento sia effettuato con mezzi automatizzati.**
2. **….l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.**

77

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL FRAMEWORK DI RIFERIMENTO

78

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL FRAMEWORK

79

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

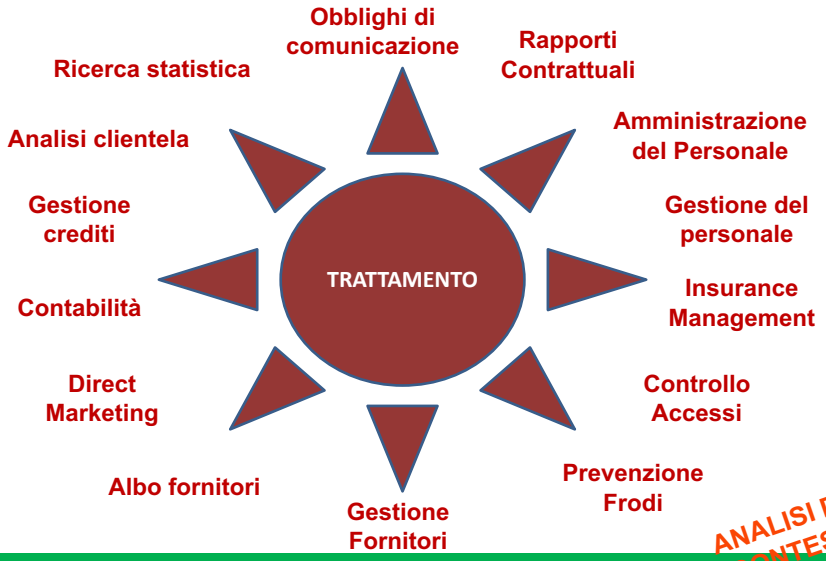
CATEGORIE DI TRATTAMENTO

L'articolo 4 definisce il trattamento dei dati personali come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali

80

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LE FINALITA' DEL TRATTAMENTO

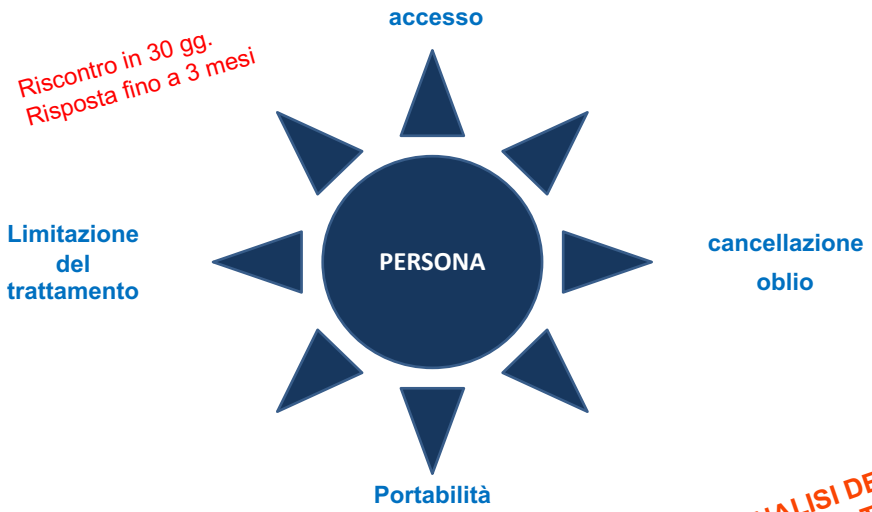


ANALISI DEL CONTESTO

81

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

I DIRITTI DELL'INTERESSATO



ANALISI DEL CONTESTO

82

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA MAPPA DEL SISTEMA: IL REGISTRO DEI TRATTAMENTI

DA ART. 30 (IL REGISTRO DEL TRATTAMENTO…)

1. **Ogni titolare del trattamento e ogni rappresentante deve tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Il registro contiene**

a) il nome e i dati di contatto del titolare del trattamento e, del contitolare se presente, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; CHI LO FA?

b) le finalità del trattamento; PERCHE'?

c) descrizione delle categorie di interessati e delle categorie di dati personali; DI QUALI INTERESSATI'?

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; A CHI COMUNICO?

e) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, e documentazione delle garanzie adeguate; TRASFERISCO ALL'ESTERO?

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

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzati- ve di cui all'articolo 32, paragrafo 1. COME LI PROTEGGO?

83

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA MAPPA DEL SISTEMA: IL REGISTRO DEI TRATTAMENTI

Unità Organizzativa	Categoria di trattamento	Finalità del trattamento	Software, Database, Manutenzione	Denominazione e dati di contatto del contitolare (se presente)
amministrazione	raccolta	Selezione personale	Gestione organizzativa	
hr	registrazione	Assunzione personale	Gestione contabile	
produzione	uso	Gestione registro clienti	Gestione tecnica	
vendite	adattamento	Gestione albo fornitori	Gestione commerciale	
tecnico	estrazione	Preventivi clienti	Server fisici	
security	modifica	marketing	Cloud	
	cancellazione	Customer care	Manutenzione fisica	
	distruzione	Sicurezza fisica/controllo accessi/ security	Manutenzione da remoto	

84

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA MAPPA DEL SISTEMA: IL REGISTRO DEI TRATTAMENTI

Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Denominazione responsabili esterni (se presenti)	Paesi Terzi o organizzazioni internazionali verso cui i dati possono essere trasferiti
Interessati selezione Collaboratori/dipendenti Referenti fornitori Referenti clienti aziendali Clienti privati visitatori passanti	di identificazione; Stile di vita; Curriculum Vitae Dati sulla salute fisica Dati sulla salute mentale Medicina del lavoro Appartenenza sindacale Particolari categorie di dati Registrazione accessi e dati di navigazione Dati di identificazione elettronica/ dati di identificazione biometrica dati di geolocalizzazione, immagini	Consulente del Lavoro, Commercialista, INPS, Assicurazioni Forze di polizia/ magistratura	Responsabile Manutenzione Software; Consulente del lavoro, Commercialista, Assicuratore,	

85

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA MAPPA DEL SISTEMA: IL REGISTRO DEI TRATTAMENTI

Indicazione garanzie adottate per il trasferimento internazionale (se applicabile)	Periodo di conservazione dei dati (se possibile)	Descrizione generale delle misure di sicurezza adottate (se possibile)	Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)
	3 anni (es. dati selezioni) 10 anni (es. documenti contabili) 2 anni (es. preventivi commerciali) Referenti clienti aziendali Clienti privati visitatori passanti	Richiamo con codici	consenso dell'interessato; esercizio di diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro necessario all'esecuzione del contratto legittimo interesse (protezione della proprietà)	consenso dell'interessato/ Trattamento ex art. 9 lett. d) GDPR

86

LA MAPPA DEL SISTEMA: IL REGISTRO DEI TRATTAMENTI

Tipologia di trattamento	Fonte dei dati personali (se applicabile)	Consenso degli Interessati	Modalità di conservazione dei dati	VALUTAZIONE DI IMPATTO
normale	CV interessato; form di adesione Telecamere/ Impianti/ Amministrazione Clienti/ Amministrazione Fornitori Sistemi informatici	Documentato: Firma su form adesione cartaceo compilato per presa visione e accettazione trattamenti e loro finalità, diritti dell'interesssato e rimando a procedure per esercizio dei diritti Documentato: richiesto alla firma del contratto Documentato: informativa su posta elettronica e internet	Digitale cartaceo	

87

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

SECURITY PRIVACY E DATA PROTECTION

88

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DA ART. 32 (LA SICUREZZA DEI TRATTAMENTI…)

1) Tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità, 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:
   a) la pseudonimizzazione e la cifratura dei dati personali;
   b) la capacità di assicurare su base permanente la riservatezza, l' integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2) Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3) L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4) ….fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

89

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DA ART. 35 (LA VALUTAZIONE DI IMPATTO…)

1) Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2) Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3) in particolare nei casi seguenti:
   a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
   b) trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
   c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

90

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DA ART. 35 (LA VALUTAZIONE DI IMPATTO…)

4) **L' autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L' autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.**

5) **L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto.**

6) **….**

7) **La valutazione deve contenere almeno:**

   a) **una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;**

   b) **una valutazione della necessità e proporzionalistà dei trattamenti in relazione alle finalità;**

   c) **una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;**

   d) **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.**

91

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DA ART. 33 (NOTIFICA DI VIOLAZIONE ALL'AUTORITA' DI CONTROLLO…)

1) **In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all' autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.**

2) **Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.**

3) **La notifica DEL TITOLARE deve almeno:**

   a) **descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;**

   b) **comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;**

   c) **descrivere le probabili conseguenze della violazione dei dati personali;**

   d) **descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.**

4) **Qualora non sia possibile fornire le informazioni contestualmente, possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.**

5) **Il titolare del trattamento documenta qualsiasi violazione, comprese le circostanze, le sue conseguenze e i provvedimenti per porvi rimedio.**

92

DA ART. 34 (NOTIFICA DI VIOLAZIONE ALL'INTERESSATO…)

1) **Se la violazione può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.**
2) **Gli comunica con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).**
3) **Non è richiesta la comunicazione all'interessato se :**
    1) **il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate (EFFICACI) di protezione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;**
    2) **ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;**
    3) **detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.**

93

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

(LA PSEUDONIMIZZAZIONE…)

Consiste nel trattare i dati personali perché questi non possano più essere attribuiti a un interessato specifico, senza l'utilizzo di informazioni aggiuntive,

tali informazioni aggiuntive devono essere conservate separatamente ed essere assoggettate a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

94

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

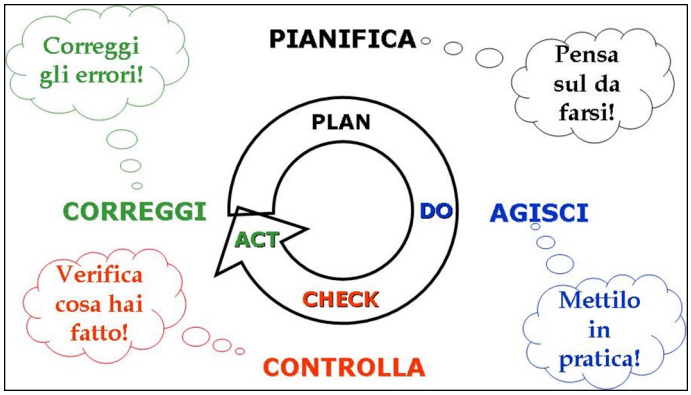
DATA PROTECTION E SECURITY

95

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION: IL PROCESSO DI SECURITY

- ***Modello PDCA o Ciclo di Deming:*** strumento operativo molto utile nell'approccio processuale alla Security, che è anche alla base di qualsiasi sistema di gestione



96

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA VALUTAZIONE DEL RISCHIO PER LA PIA

COME VALUTO IL RISCHIO?

COME DIMOSTRO DI AVER RIDOTTO IL RISCHIO

VALUTAZIONE PREVENTIVA (SENZA MISURE DI OPPOSIONE)

VALUTAZIONE POTENZIALE (CON MISURE DI OPPOSIZIONE)

DIMOSTRAZIONE «BY DESIGN» DI ESSERE IN GRADO DI SVOLGERE I TRATTAMENTI CON UN LIVELLO «ACCETTABILE» DI RISCHIO OTTENIBILE CON LE GIUSTE MISURE DI OPPOSIZIONE/PROTEZIONE

97

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION: IL PROCESSO DI SECURITY

ANALISI DEL CONTESTO	MISURAZIONE RISCHIO PREVENTIVO	MISURAZIONE RISCHIO POTENZIALE	MISURAZIONE RISCHIO EFFETTIVO
	T^0	T^1	T^2
Azienda Dati Processi Trattamenti Finalità DEFINIZIONE POLITICHE ORGANIZZAZIONE	Misurazione del Rischio alla luce della capacità delle misure esistenti di opporsi alle minacce, per la realizzazione in sicurezza del trattamento e riduzione della probabilità di impatto nei confronti dell'interessato	Stima del Rischio alla luce della capacità potenziale delle misure esistenti ottimizzate e dell'introduzione di nuove misure, per la realizzazione in sicurezza del trattamento, e riduzione della probabilità di impatto nei confronti dell'interessato	Misurazione del Rischio alla luce della capacità dimostrata dalle misure esistenti ottimizzate e dell'introduzione di nuove misure, nella realizzazione in sicurezza del trattamento., e di ridurre la probabilità di impatto nei confronti dell'interessato

98

DATA PROTECTION: IL PROCESSO DI SECURITY

- ***Rischio:*** **il rischio è l'effetto di fattori interni ed esterni e di altre influenze che rendono incerto il raggiungimento degli obiettivi delle organizzazioni (di ogni tipo e dimensione). Il rischio è spesso espresso come combinazione degli effetti di un evento e le probabilità associate di accadimento.**

R = P X D

R= rischio P= probabilità D= impatto/danno economico

Magnitudo del singolo rischio

Scala delle priorità

99

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

L'IMPATTO SULLA PERSONA PER VALUTARE IL RISCHIO DEL TRATTAMENTO

100

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION: IL PROCESSO DI SECURITY

- La ***probabilità di accadimento*** a sua volta è funzione della frequenza e della vulnerabilità

P = F(f ;V)

P= probabilità **f**= frequenza **V**= vulnerabilità

È funzione di:
- **Accadimenti precedenti**
- **Efficacia misure implementate**

È funzione di:
- **Grado adeguatezza procedure**
- **Grado efficienza tecnologie**
- **Grado adeguatezza risorse umane**
- **Grado implementazione misure di compliance**

101

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION: UN PROCESSO DI SECURITY

ESPOSIZIONE	MINACCIA	VULNERABILITA'	RISCHIO
			
Dato	Furto Manipolazione Cancellazione Diffusione non autorizzata Esercizio diritto	Assenza o poca efficacia delle misure	Compliance Economico (sanzione) (Risarcimento) Penale

102

IL FILO LOGICO DEL RISCHIO: L'ESPOSIZIONE

- quantità misurabile di bene materiale o immateriale potenzialmente soggetto al danno (n. di abitanti, n. di persone di un eventi, ettari di bosco, n. di vetture, gigabyte di dati etc.
- **= tutto ciò che il Professionista della security deve tutelare**
- **= il dato personale**

103

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL FILO LOGICO DEL RISCHIO: LA MINACCIA

rappresenta la possibilità che……

- venga tentato un attacco
- avvenga un incidente
- si manifesti un evento naturale
- si manifesti un comportamento violento
- **vi sia una innovazione normativa**
- vi sia un cambiamento non controllabile nell'ambiente circostante
- **Si tratti un dato personale**

104

IL FILO LOGICO DEL RISCHIO: LA VULNERABILITA'

- Debolezza di una di una organizzazione rispetto ad una minaccia, inversamente proporzionale alla efficacia delle misure messe in atto per contrastarla
  - **Un archivio fisico di facile accesso**
  - **Un server non protetto**
  - **La mancanza di una rete «guest»**
  - **Il via vai di pen drive**
  - **La presenza di immagini sul website**

105

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

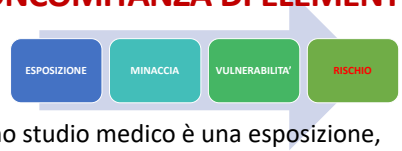
IL FILO LOGICO DEL RISCHIO: IL RISCHIO

- la "*minaccia*" (**accesso a dato personale da parte di malintenzionato**)
- può insistere su di una "esposizione", (**dato personale**)
- e sfruttare, ovvero avvalersi delle debolezze, o "*vulnerabilità*" di una organizzazione (**faldoni medico di famiglia esposti in archivio aperto**),
- inducendo il generarsi di un "*danno*" (**diffusione dato sanitario con impatto sull'interessato e sull'Organizzazione che avrebbe dovuto tutelarlo, sul titolare e sul DPO**),
- ed esponendo in tal senso l'Interessato e l'Organizzazione al "*rischio*" (**danno causato all' interessato e danno causato all'Organizzazione)** riducendone la "*sicurezza*".
- La combinazione di minaccia esposizione vulnerabilità può generare il rischio che può poi concretizzarsi in danno.

106

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL FILO LOGICO DEL RISCHIO: CONCOMITANZA DI ELEMENTI



- un dato sanitario di Tizio nell'archivio di uno studio medico è una esposizione, ma lo studio medico non è automaticamente soggetto ad un rischio esplicito;
- Il malintenzionato alla ricerca di informazioni per mettere in difficoltà Tizio è in sé è una minaccia ma non necessariamente sfocia in un danno;
- I Faldoni esposti in Archivio con indicazioni di ordine dei cognomi da A a Z sono una vulnerabilità ma non per forza generano una acquisizione illecita del dato di Tizio.
- Il rischio di uso illecita del suo dato Sanitario può generare un danno per Tizio quando il suo dato è esposto alla minaccia dell'accesso da parte del malintenzionato che incontra la vulnerabilità data dalla facilità di accesso al dato su Archivio aperto, che diffonde quel dato arrecando un danno all'interessato e di conseguenza all'Organizzazione.

107

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA CASSETTA DEGLI ATTREZZI DEL PROFESSIONISTA E DEL DPO

- **MISURE PASSIVE**: implementate per reagire al concretizzarsi di una minaccia per lo più agendo sul contesto, al fine di aumentare il tempo di cui la minaccia ha bisogno per produrre il danno nella sua consistenza caratteristica (tempo di ritardo vantaggiosamente utilizzabile per neutralizzare/ridurre il danno);
- ***difese fisiche e strutturali, non danno segnalazioni di allarme ma servono per ritardare il tempo di attacco e di superamento delle stesse barriere***

108

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA CASSETTA DEGLI ATTREZZI DEL PROFESSIONISTA E DEL DPO

- **MISURE ATTIVE**: implementate per evidenziare tempestivamente il sorgere della minaccia che produrrà il danno, attraverso la modificazione dell'equilibrio stabilito (sistemi di monitoraggio del traffico di rete per cogliere anomalie, telecamere per cogliere modifiche dei pixel di riferimento, sistemi di allarme sensibili alle prime vibrazioni, rilevatori di fumo sensibili ai primi fumi ancora invisibili). La misura è finalizzata ad evidenziare tempestivamente l'inizio dell'evento negativo al fine di utilizzare vantaggiosamente il tempo disponibile prima del manifestarsi del danno, per porre in essere contromisure che ne evitino, nel limite del possibile, la concretizzazione stessa o almeno ne riducano la consistenza.
- ***Le misure attive, o elettroniche, sono le tecnologie basate principalmente sull'elettronica e gestite da una centrale di acquisizione allarmi, che danno una segnalazione di allarme, senza opporsi fisicamente ad attacchi o effrazioni, e quindi sono elemento fondamentale per attivare tempestivamente le contromisure all'evento (sensori volumetrici e a infrarossi, per esterno e per interno, microonde, sistemi interrati, varie tipologie di sistemi di allarme perimetrale, sistemi antitaccheggio, ecc.)***

109

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA CASSETTA DEGLI ATTREZZI DEL PROFESSIONISTA E DEL DPO

- **MISURA ORGANIZZATIVE**: predisposte in base alla valutazione logica di efficacia delle Misure Passive ed Attive al fine di integrare le stesse con una specifica azione oppositiva avente l'obiettivo di riduzione massima del danno utilizzando il tempo reso disponibile dalle stesse misure Attive o Passive applicate al contesto.
- ***Le misure organizzative sono tutte quelle che presuppongono azioni o interventi finalizzati ad evitare il danno conseguente al rischio trattato (norme e procedure, comportamenti e precauzioni, istruzioni e divieti, corsi di informazione e formazione, piano e procedure di intervento emergenza, organizzazione di primo soccorso e intervento, comunicazione e gestione dello stato di emergenza, coinvolgimento delle Forze esterne, gestione dello sfollamento e dell'evacuazione, ecc.)***
- **MISURE DI COMPLIANCE:** procedure e linee guida stabilite dal GDPR e da progettare e implementare all'interno dell'Organizzazione
- Framework di riferimento, registro dei trattamenti etc
- Consultazione Preventiva, Adozione codici di condotta, Certificazioni

110

DATA PROTECTION E SECURITY

ANOMALIE

- Se devo effettuare la PIA per i trattamenti che presentano i rischi più elevati, come faccio a stabilire prima di valutarli quali siano i rischi più elevati?
- Non sarebbe meglio parlare di valutazione obbligatoria del rischio per quei trattamenti che presentano impatti potenziali più elevati?
- Ed in tal senso come stabilisco l'entità dell'impatto sulla persona a seguito di un accadimento di violazione dei suoi diritti, o di uso improprio dei suoi dati personali che ha portato ad una conseguenza negativa nei suoi confronti?
- Quali sono tali conseguenze negative?

111

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

PROVIAMO A METTERE UN PO' D'ORDINE

IMPATTO/DANNO → **CONSEGUENZA NEGATIVA POTENZIALE SULLA PERSONA PER IL CONCRETIZZARSI DI UN RISCHIO DOVUTO ALLA MANIFESTAZIONE DI UNA MINACCIA CHE HA SFRUTTATO LA VULNERABILITA' DELL'ORGANIZZAZIONE CHE HA EFFETTUATO QUEL PARTICOLARE TRATTAMENTO**

↓

SE LA CONSEGUENZA NEGATIVA POTENZIALE SULLA PERSONA CHE PUO' ESSERE INDOTTA DALLO SVOLGIMENTO DI UN DETERMINATO TRATTAMENTO E' «IMPORTANTE» E' NECESSARIO SVOLGERE UNA PREVALUTAZIONE DEL RISCHIO FINALIZZATA A COMPRENDERE SE L'ORGANIZZAZIONE E' ATTREZZATA PER SVOLGERE QUEL TRATTAMENTO RIDUCENDO AL PASSIMO LA POSSIBILITA' CHE QUESTA CONSEGUENZA SI VERIFICHI

112

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME FACCIO A QUANTIFICARE L'IMPATTO

IMPATTO/DANNO → CONSIDERANDO
ART. 35
GRUPPO ART. 29
DECISIONI/ LINEE GUIDA GARANTE

↓

RISPETTO A OBBLIGO O MENO DI PIA

MA PER VALUTARE IL RISCHIO PREVENTIVO E PER STABILIRE A PRIORI SE L'ORGANIZZAZIONE E' IN CONDIZIONI DI IMPLEMENTARE QUEL TRATTAMENTO DEVO DARE UNA DIMENSIONE ALL'IMPATTO E DEVO OMOGENEIZZARE LE MISURE PER IL CALCOLO DELLA MAGNITUDO DEL RISCHIO

R=PXD

113

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LA VALUTAZIONE D'IMPATTO SECONDO ENISA (AGENZIA EUROPEA PER CYBERSECURITY)

il titolare / responsabile del trattamento deve valutare il potenziale impatto sui diritti e sulle libertà delle persone che potrebbe essere generato da un breach del sistema di gestione dei dati

VIOLAZIONE DELLA RISERVATEZZA

VIOLAZIONE DELLA INTEGRITA'  VIOLAZIONE DELLA DISPONIBILITA'

particolari caratteristiche del titolare / responsabile del trattamento

particolari caratteristiche degli interessati

volume dei dati personali

tipologia

criticità dell'operazione di trattamento

livello di identificabilità degli interessati

114

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME STRUTTURO UNA VALUTAZIONE DI IMPATTO

QUALIFICO L'ESPOSIZIONE

115

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

	ESPOSIZIONE			
CATEGORIA DI TRATTAMENTO	PERSONE COINVOLTE	PERSONE E APPARECCHIATURE COINVOLTE	DATI PERSONALI COINVOLTI	FINALITA' DEL TRATTAMENTO
VIDEOSORVEGLIANZA PRESSO CLIENTI	CLIENTI FORNITORI DIPENDENTI MANAGEMENT TERZI PASSANTI	SERVER SALA OPERATIVA	IMMAGINI DATI BIOMETRICI	SICUREZZA SEDE OPERATIVA
		PC SALA OPERATIVA (windows+linux)		
		PC VIRTUALE		
		GUARDIE GIURATE DI TURNO IN SALA OPERATIVA		

116

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME STRUTTURO UNA VALUTAZIONE DI IMPATTO

QUANTIFICO L'IMPATTO POTENZIALE DEL TRATTAMENTO SULL'INTERESSATO

- PROPORZIONALITA'/ INVASIVITA' DEL TRATTAMENTO
- CONSEGUENZE POTENZIALI NEGATIVE DI TIPO ECONOMICO
- CONSEGUENZE POTENZIALI NEGATIVE DI TIPO LAVORATIVO
- CONSEGUENZE POTENZIALI NEGATIVE DI TIPO REPUTAZIONALE
- CONSEGUENZE POTENZIALI NEGATIVE DI TIPO SANITARIO SULL'INTERESSATO

ENISA quattro livelli di impatto basati su dati soggettivi:

BASSO: le persone possono incontrare alcuni piccoli inconvenienti che supereranno senza problemi (reinserimento dati, tempo perso per blocco procedure, etc)

MEDIO: gli individui in media possono incontrare notevoli inconvenienti che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, blocco procedure, stress, etc)

ALTO: gli individui possono incontrare conseguenze significative che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera pagatori, perdita del lavoro, posizioni di garanzia,etc)

MOLTO ALTO: conseguenze gravi ed irreversibili che potrebbero non essere superate (incapacità lavorativa, disturbi psicologici o fisici, etc)

117

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IMPATTO POTENZIALE SU PERSONA						
PROPORZIONALITA'/ INVASIVITA'	ECONOMICO	REPUTAZIONALE	SANITARIO	LAVORATIVO	IMPATTO MEDIO	IMPATTO MEDIO CLASSIFICATO
5	5	5	1	5	4,2	4

118

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME STRUTTURO UNA VALUTAZIONE DI IMPATTO

IDENTIFICO LE MINACCE

119

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

MINACCIA	AZIONI DI MIGLIORAMENTO INDIVIDUATE A T0 (25 MAGGIO 2018)
M1 . MANCATA COMPLIANCE E VIOLAZIONE DIRITTI	DEFINIZIONE E IMPLEMENTAZIONE PROCEDURE SCRITTE ATTUAZIONE FRAMEWORK DI RIFERIMENTO COMPILAZIONE E AGGIORNAMENTO PERIODICO REGISTRO TRATTAMENTO FORMAZIONE DI BASE E AGGIORNAMENTO CONTINUO DEL PERSONALE
M2 - ACCESSO ILLEGITTIMO AI DATI	PREDISPOSIZIONE DI PROGRAMMA PER AGGIORNAMENTO MANUTENZIONE E TEST DELLE MISURE DEFINIZIONE DELLE PROCEDURE E DELLE RESPONSABILITA
M3 - MODIFICHE INDESIDERATE DEI DATI	
M4 - PERDITA DEI DATI	

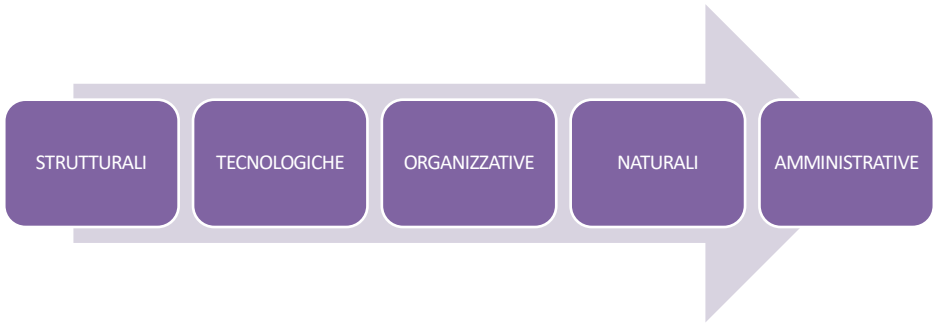
120

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME STRUTTURO UNA VALUTAZIONE DI IMPATTO

IDENTIFICO LE VULNERABILITA' DEL CONTESTO RISPETTO ALLA TIPOLOGIA DI TRATTAMENTO ED ALLE MINACCE INDIVIDUATE



121

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

VULNERABILITA' MEDIA RILEVATA	VULNERABILITA' MEDIA CLASSIFICATA	FREQUENZA MEDIA STIMATA	FREQUENZA MEDIA CLASSIFICATA	PROBABILITA'	MAGNITUDO RISCHIO GENERATO DAL TRATTAMENTO
2,037676768	3	2,875	4	3,5	14

122

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME STRUTTURO UNA VALUTAZIONE DEL RISCHIO CHE TENGA CONTO DEL LIVELLO DI IMPATTO GENERATO DAL TRATTAMENTO

VALUTO L'EFFICACIA DELLE MISURE PRESENTI, DI OPPOSIZIONE ALLE MINACCE CHE INCIDONO SULLE ESPOSIZIONI, E POTREBBERO SFRUTTARE LE VULNERABILITA' DEL CONTESTO RISPETTO ALLA TIPOLOGIA DI TRATTAMENTO

MISURE PER RAFFORZARE I DIRITTI FONDAMENTALI
- INFORMATIVE
- PROCEDURE RICHIESTA E VALUTAZIONE DIRITTI PERSONA
- DECLINAZIONE CHIARA RUOLI E RESPONSABILITA'
- AZIONI VERIFICA CONSENSI TRATTAMENTO (OVE NECESSARI)
- AZIONI VERIFICA BASI LEGALI TRATTAMENTO
- EFFICACIA MEDIA

MISURE A TUTELA DEL CICLO DI VITA DEL DATO
- MISURE PASSIVE
- MISURE ATTIVE
- MISURE ORGANIZZATIVE

123

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Peso su efficacia di opposizione	1) Misure a rafforzare i diritti fondamentali		TRATTAMENTO DI RIFERIMENTO	MINACCIA DI RIFERIMENTO
0,4	1.1	Informative Preventivi	T3	M1
	1.2	Informative Contratti fornitori	T3	M1
	1.3	Informative Contratti dipendenti	T1 T2 T3	M1
	1.4	Informative Sito Web	T1 T2 T3	M1
	1.5	Informative Visitatori Sede	T1 T2 T3	M1 - M2
	1.6	Informative Passanti prossimità perimetro aziendale	T2	M1
	1.7	Procedure per la richiesta e la valutazione dei diritti della persona	T1 T2 T3	M1
	1.8	Declinazione formale e chiara di ruoli e responsabilità: nomina responsabile protezione dati	T1 T2 T3	M1
	1.9	Declinazione formale e chiara di ruoli e responsabilità: nomina per iscritto responsabili esterni	T1 T2 T3	M1
	1.10	Declinazione formale e chiara di ruoli e responsabilità: nomina per iscritto referenti interni	T1 T2 T3	M1
	1.11	Azioni di verifica dei consensi del trattamento (OVE NECESSARI)	T1 T2 T3	M1
	1.12	Azioni di verifica delle basi legali del trattamento	T1 T2 T3	M1
	1.13			
	1.14			

124

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

	2) Misure a tutela del ciclo di vita del dato, a garanzia della effettuazione dei trattamenti in sicurezza			
	2) Misure Attive			
0,2	2.1	Sistema di videosorveglianza esterna	T1 T2 T3	M2 - M3 - M4
	2.2	Sistema di videosorveglianza interna	T1 T2 T3	M2 - M3 - M4
	2.3	Sistema d'allarme volumetrico	T1 T2 T3	M2 - M3 - M4
	2.4	Sistema d'allarme perimetrico	T1 T2 T3	M2 - M3 - M4
	2.5	tracciamento accessi a singole caselle mail	T1 T2 T3	M2 - M3 - M4
	2.6			
	2.7			
	3) - Misure Passive:			
0,2	3.1	Autenticazione per accesso a PC e applicativi	T1 T2 T3	M2 - M3 - M4
	3.2	Separazione server dati amministrazione	T3	M2 - M3 - M4
	3.3	doppio firewall server dati centrale operativa	T1 T2	M2 - M3 - M4
	3.4	firewall server aree amministrative tecnica e commerciale	T3	M2 - M3 - M4
	3.5	firewall server sede distaccata	T1 T2 T3	M2 - M3 - M4
	3.6	antivirus s	T1 T2 T3	M2 - M3 - M4
	3.7	back up disaster recovery	T1 T2 T3	M2 - M3 - M4
	3.8	intrusion detection	T1 T2 T3	M2 - M3 - M4
	3.9	vulnerability assessment/penetration test	T1 T2 T3	M2 - M3 - M4
	3.10	cifratura dei dati	T1 T2	M2 - M3 - M4
	3.11	macchina distruggi documenti	T3	M2 - M3 - M4
	3.12	Cassaforte in stanza chiusa e allarmata	T1 T2 T3	M2 - M3 - M4
	3.13	Armadi chiusi in stanza chiusa e allarmata	T3	M2 - M3 - M4
	3.14	IP statici	T1 T2 T3	M2 - M3 - M4
	3.15	isolamento/non presenza WI FI	T1 T2 T3	M2 - M3 - M4
	3.16			

125

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

	4) - Misure organizzative:			
0,2	4.1	istruzioni a tutto il personale per il trattamento dei dati	T1 T2 T3	M1 - M2
	4.2	accesso controllato e limitato a spazi fisici e virtuali di conservazione	T1 T2 T3	M2 - M3 - M4
	4.3	procedure per la chiusura degli armadi e dell'accesso agli spazi di conservazione	T1 T2 T3	M2 - M3 - M4
	4.4	procedura modifica periodica credenziali	T1 T2 T3	M2 - M3
	4.5	policy aziendali	T1 T2 T3	M1 - M2 - M3
	4.6	formazione continua	T1 T2 T3	M1 - M2 - M3
	4.7	procedure per business continuity e disaster recovery	T1 T2 T3	M2 - M3
	4.8	divieto di inserimento dati personali dei clienti su cellulari aziendali e o privati	T1 T2 T3	M2 - M3
	4.9	divieto utilizzo dispositivi di memoria su pc e desk aiendali	T1 T2 T3	M2 - M3
	4.10	divieto di accesso a locali archivio dati personali ai non autorizzati	T3	M2 - M3
	4.11	Procedura di accesso con autenticazione biometrica alle strutture da parte responsabili azienda	T1 T2 T3	M2 - M3
	4.12	Procedura di accesso per i non autenticati e per le merci	T1 T2 T3	M2 - M3
	4.13	Procedure registrazione dati in sicurezza	T1 T2 T3	M1 - M2 - M3
	4.14	Procedure archiviazione dati in sicurezza	T1 T2 T3	M1 - M2 - M3
	4.15	Procedure estrazione dati in sicurezza	T1 T2 T3	M1 - M2 - M3
	4.16	Procedure cancellazione dati in sicurezza	T1 T2 T3	M1 - M2 - M3
	4.17	Procedure trasporto documenti controllo accessi in sicurezza	T1 T2 T3	M1 - M2 - M3
	4.18	Procedure distruzione documenti in sicurezza	T1 T2 T3	M1 - M2 - M3
	4.19	Procedura periodica ripristino password	T1 T2 T3	M2 - M3
	4.20	Procedura accesso a casella mail operativa in caso di indisponibilità titolare	T3	M1 - M2
	4.21	Guardie giurate armate	T1 T2 T3	M2 - M3
	4.22	briefing semestrale	T1 T2 T3	M2 - M3

126

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME FACCIO A QUANTIFICARE L'IMPATTO

IMPATTO/DANNO → D/I=F(I;E;L;R;S)

D/I=MEDIA(2;3;4;5;2)=

D/I=MEDIA POND(0,1*2;0,25*3;0,25*4;0,2*5;0,2*2)=3,35

IPOTESI: IMPATTO DEL TRATTAMENTO FUNZIONE DELLA INVASIVITA' DEL TRATTAMENTO E CONSEGUENZE POTENZIALI NEGATIVE DI TIPO ECONOMICO, LAVORATIVO, REPUTAZIONALE, SANITARIO SULL'INTERESSATO.

R=PXD

127

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME FACCIO A QUANTIFICARE IL RISCHIO: LA PROBABILITA'

PROBABILITA' → P=F(V;F)

P=MEDIA(V;F)

P=MEDIA POND(V;F)

IPOTESI: CONSIDERO LA COMPONENTE PROBABILITA' DELLA FORMULA DEL CALCOLO DEL RISCHIO COME FUNZIONE DI VULNERABILITA" E FREQUENZA

R=PXD

128

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DATA PROTECTION E SECURITY

COME FACCIO A QUANTIFICARE IL RISCHIO: LA VULNERABILITA'

VULNERABILITA' → **F=Vmax-(Er)**

IPOTESI: CONSIDERO LA VULNERABILITA' COME FUNZIONE INVERSA DELL'EFFICACIA DELLE MISURE CHE HO A DISPOSIZIONE; LA VULNERABILITA' RELATIVA DEL TRATTAMENTO LA CONSIDERO COME VULNERABILITA' RESIDUA DERIVANTE DALLA SOTTRAZIONE TRA VULNERABILITA' MASSIMA E EFFICACIA RELATIVA DELLE MISURE MESSE IN ATTO.
MAGGIORE SARA' L'APPORTO DI EFFICACIA MINORE LA VULNERABILITA' RESIDUA

129

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

efficacia dimostrata in contesti e situazioni analoghe rispetto alla specifica minaccia o da certificazioni conformità e standard	l'effettivo funzionamento della misura in termini di come risultato atteso rispetto al contesto	di compliance normative, di software gestionali ed operativi, o a supporto di sistemi di sicurezza, alla luce di nuove normative, di nuovi patch o release, di nuove procedure da implementare etc	previsti dalle normative o dal costruttore, secondo il piano concordato con organizzazione e fornitori	previsti anche dalle normative o dal costruttore, e inseriti in un piano concordato tra organizzazione e fornitori CERTIFICAZIONI/AUDIT		
FUNZIONALITA'	EFFICIENZA	AGGIORNAMENTO	MANUTENZIONE	TEST /AUDIT		
tra 1 e 5 per definire capacità risolutiva delle misure nel contesto rispetto alla minaccia considerata	tra 1 e 5 per definire una misura da non performante fino a perfettamente performante	tra 1 e 5 per definire da non aggiornato fino a completamente aggiornato	tra 1 e 5 per definire da mai effettuati, a effettuati in modo perfettamente conforme al piano di manutenzione previsto	tra 1 e 5 per definire da previsti e mai effettuati, a effettuati in modo perfettamente conforme al programma di test concordato	EFFICACIA MEDIA	VULNERABILITA' MEDIA STIMATA (VULNERABILITA' MASSIMA=5- EFFICACIA MEDIA)
4	2	2	2	2	2,4	2,6
4	2	2	2	2	2,4	2,6
4	2	2	2	2	2,4	2,6

	RISCHIO DA MINACCIA 1 : MANCATA COMPLIANCE E VIOLAZIONE DIRITTI			RISCHIO DA MINACCIA 2: ACCESSO ILLEGITTIMO AI DATI			RISCHIO DA MINACCIA 3: MODIFICHE INDESIDERATE DEI DATI			RISCHIO DA MINACCIA 4: PERDITA DEI DATI		
	ACCADIMENTI AZIENDALI ULTIMI 5 ANNI (PESO DA 1 A 5)	ACCADIMENTI MEDI SETTORE ULTIMI 5 ANNI (PESO DA 1 A 5)	MISURA FREQUENZA RELATIVA T0	ACCADIMENTI AZIENDALI ULTIMI 5 ANNI (PESO DA 1 A 5)	ACCADIMENTI MEDI SETTORE ULTIMI 5 ANNI (PESO DA 1 A 5)	MISURA FREQUENZA RELATIVA T0	ACCADIMENTI AZIENDALI ULTIMI 5 ANNI (PESO DA 1 A 5)	ACCADIMENTI MEDI SETTORE ULTIMI 5 ANNI (PESO DA 1 A 5)	MISURA FREQUENZA RELATIVA T0	ACCADIMENTI AZIENDALI ULTIMI 5 ANNI (PESO DA 1 A 5)	ACCADIMENTI MEDI SETTORE ULTIMI 5 ANNI (PESO DA 1 A 5)	MISURA FREQUENZA RELATIVA T0
ACCADIMENTO RISCHIO 1	4	5	4,5	1	3	2	2	3	2,5	2	3	2,5
PESO	0,5	0,5		0,5	0,5		0,5	0,5		0,5	0,5	

130

LE SANZIONI PER LA CATTIVA GESTIONE DEI DATI PERSONALI

131

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LE SANZIONI PER LA MALA GESTIO DEI DATI PERSONALI

- Le sanzioni Privacy in Italia sono le stesse di quelle applicate al resto d'Europa, con la prerogativa di essere ponderate in base a:
  - tipo di violazione;
  - gravità della violazione:
  - durata della violazione.
- Dal 1 gennaio al 17 agosto in tutta l'Unione Europea hanno superato i 60 milioni di euro (60.181.250).
- Tra le infrazioni più spesso rilevate si sottolineano: trattamenti illeciti di dati personali (quasi nella metà dei casi); adozione di misure di sicurezza insufficienti o non adatte; inadeguatezza o carenza delle informative; violazione dei diritti degli interessati e mancato rispetto delle disposizioni in materia di violazione dei dati (Data Breach).

132

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

LE SANZIONI PER LA MALA GESTIO DEI DATI PERSONALI

	Controller	Country	Fine [€]	Type of Violation	Date
1	**British Airways**	UNITED KINGDOM	204,600,000	Insufficient technical and organisational measures to ensure information security	08 Jul 2019
2	**Marriott International, Inc**	UNITED KINGDOM	110,390,200	Insufficient technical and organisational measures to ensure information security	09 Jul 2019
3	**Google Inc.**	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
4	**TIM (telecommunications operator)**	ITALY	27,800,000	Insufficient legal basis for data processing	15 Jan 2020
5	**Austrian Post**	AUSTRIA	18,000,000	Insufficient legal basis for data processing	23 Oct 2019
6	**Wind Tre S.p.A.**	ITALY	16,700,000	Insufficient legal basis for data processing	13 Jul 2020
7	**Deutsche Wohnen SE**	GERMANY	14,500,000	Non-compliance with general data processing principles	30 Oct 2019
8	**Telecoms provider (1&1 Telecom GmbH)**	GERMANY	9,550,000	Insufficient technical and organisational measures to ensure information security	09 Dec 2019
9	**Eni Gas e Luce**	ITALY	8,500,000	Insufficient legal basis for data processing	11 Dec 2019
10	**Google LLC**	SWEDEN	7,000,000	Insufficient fulfilment of data subjects rights	11 Mar 2020

133

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante vs Comune di Roma e ATAC

La società **Atac spa,** incaricata dal Comune anche per la gestione dei parcheggi, aveva avviato un **aggiornamento tecnologico dei parcometri per offrire nuovi servizi** (ad esempio il pagamento di sanzione/tributi o l'acquisto/rinnovo dei titoli del trasporto pubblico) e per **introdurre nuove modalità di pagamento, inserendo anche il numero di targa del veicolo.** Parte della strumentazione era stata fornita da un'altra società, la **Flowbird Italia srl** (ex Parkeon srl). Tutte le informazioni relative alla sosta venivano poi gestite attraverso un sistema centralizzato al quale poteva accedere, tramite un'apposita app, anche il personale incaricato di controllare il pagamento dei parcheggi.

l **Nucleo speciale Privacy della Guardia di finanza,** ha rilevatovarie irregolarità.

il **Comune di Roma**, in quanto titolare del trattamento, non aveva fornito alcuna informazione sul trattamento dei dati degli automobilisti, **non aveva nominato la società Atac responsabile del trattamento**, né fornito a quest'ultima le necessarie istruzioni su come trattare i dati raccolti. Neppure la società subfornitrice era stata incaricata formalmente o istruita su come procedere in merito al trattamento dei dati.

e società n**on avevano predisposto il registro dei trattamenti**

Non era stato considerato il principio della progettazione by design e by default. né erano state adottate idonee misure di sicurezza Il personale addetto, inoltre, avrebbe potuto controllare in maniera massiva e ripetuta nel tempo qualunque targa, magari per conoscere le abitudini di una persona e i luoghi di sosta, senza lasciare alcuna traccia nel sistema informativo.

il Garante per la privacy ha previsto una sanzione di 800.000 per Roma Capitale, di 400.000 per Atac spa e di 30.000 per Flowbird Italia srl. Si tratta di somme calcolate tenendo conto della **grande quantità di dati personali trattati** (da giugno 2018 a novembre 2019 il sistema di Atac Spa aveva già registrato i dati di 8.600.000 soste

134

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy francese vs Google

importo economico e mediatico in assoluto più alto (50 milioni di euro) - **sistema Android per dispositivi mobili.**

violazione degli obblighi di trasparenza e informazione: non presentava all'utenza le modalità del trattamento in modo chiaro e facilmente accessibile: informazioni essenziali quali la finalità del trattamento, il periodo di conservazione, le tipologie dei dati coinvolti, non di immediata individuazione ma sparpagliate in diversi documenti, imponendo una navigazione complicata tra link e pulsanti per accedervi.

Violazione dell'obbligo di indicare una base giuridica per il trattamento relativo alla pubblicità mirata, affinché venga reso lecito l'utilizzo di dati finalizzato alla personalizzazione dei messaggi pubblicitari.

la politica interna di Google dice che questi trattamenti si fondano sul consenso dell'interessato.

Il garante francese ha ritenuto non sia stato correttamente ottenuto per le stesse ragioni della prima sanzione; non sufficientemente informato ai sensi del GDPR e neppure specifico e chiaro.

Al creare l'*account* l'utente può modificare alcune impostazioni tramite il pulsante "più opzioni" in un menù secondario, dove la palese violazione riscontrata sono le caselline preflaggate, e che l'utente, se contrario alla profilazione pubblicitaria, dovrà procedere alla deselezione delle caselle.

elevata ma allo stesso tempo lontana dai massimali previsti dal GDPR che prevedono multe fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

135

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy austriaco vs azienda per videosorveglianza

ottobre 2018, sanzione da 4 mila euro ad una azienda per uso non appropriato sistema di video sorveglianza.

Telecamere direzionate su parte del marciapiede esterno al perimetro aziendale, al punto di riprendere i passanti in modo invasivo, senza alcuna giustificata motivazione e idonea informativa rilasciata con apposita cartellonistica.

venivano ripresi i volti dei passanti senza che essi ne fossero debitamente informati.

Il Garante privacy tedesco vs piattaforma chat online

novembre 2018, sanzionava il sito di chat online Knuddels.de, per circa ventimila euro.

violazione dell'art. 32 del GDPR: carenza di misure adeguate di sicurezza, il sito aveva subito perdite di circa due milioni di username/password e di più di ottocentomila indirizzi e–mail, recapiti di residenza degli utenti ed altri tipi di dati.

valutato positivamente il comportamento collaborativo adottato da Knuddels, perché ha provveduto ad informare immediatamente i suoi utenti e il Garante, ed introdotto modifiche alla sua infrastruttura IT per accrescere il livello di sicurezza.

136

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy portoghese vs struttura ospedaliera

importo complessivo di 400 mila euro: **accesso indiscriminato e ingiustificato di quasi seicento dipendenti ai dati sanitari dei pazienti.**

Il sistema presentava 985 utenze attive con profilo di autorizzazione per «personale medico», ma in organico erano presenti solo 296 professionisti.

trecentomila euro per il mancato rispetto della confidenzialità e per la mancata limitazione degli accessi ai dati dei soggetti ricoverati,

centomila euro per non aver garantito "su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" (art. 32 GDPR).

Contestati:

- assenza di procedura di autenticazione degli utenti del sistema informatico e relativi profili di accesso
- non corretto utilizzo dei profili e dei codici di accesso previsti nei sistemi gestionali utilizzati
- esistenza profili inattivi di utenti che non operavano più per l'azienda.

Sanzione calcolata in funzione di tipologia di dati coinvolti sulla salute di pazienti, durata della violazione, interessati coinvolti, gravità dei danni da questi subìti, negligenza nell'adozione di misure organizzative e tecniche da parte della struttura ospedaliera.

violazione considerata dolosa, perchè il titolare **aveva «consapevolmente»** collegato i profili di accesso al sistema informativo con i profili non corrispondenti, a fronte dell'utilizzo di sistemi gestionali messi a disposizione dal Ministero della Salute, di per sé erano in grado di garantire la corretta identificazione degli utenti e, limitazione degli accessi ai dati.

137

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy polacco vs società

220.000 euro per mancato rispetto dell'obbligo di informazione sancito all'art. 14 del GDPR.

trattava dati personali provenienti da fonti pubbliche per finalità commerciali

Contestata omissione di informativa a circa sei milioni di persone su al trattamento ai fini commerciali dei loro dati tratti da fonti accessibili al pubblico.

Agli interessati veniva in tal modo preclusa la possibilità di esercitare i propri diritti.

la società polacca aveva adempiuto all'obbligo di informazione solo nei confronti delle persone di cui aveva a disposizione gli indirizzi e-mail. Ritenendo di poter assolvere per gli altri tramite clausola pubblicata sul proprio sito web.

modalità di procedere ritenuta insufficiente poiché avrebbe dovuto comunicare direttamente agli interessati i loro dati personali, la fonte degli stessi, lo scopo e il periodo del trattamento previsto, nonché i diritti loro spettanti ai sensi del GDPR.

ritenuta molto grave

la condotta per carattere intenzionale della violazione (la società era a conoscenza dell'obbligo di fornire informazioni in modo diretto alle persone),

Per comportamento per niente collaborativo tenuto successivamente dalla società per porre rimedio all'infrazione

su **circa 90.000 persone informate** sul trattamento da parte dell'azienda, **più di 12.000** si sono opposti al trattamento dei loro dati

138

Il Garante privacy Danese vs società società produttrice di mobili di design

200.850 euro per aver conservato i dati di un elevato numero di clienti per un periodo superiore al necessario.

non erano stati definiti e rispettati specifici periodi di conservazione da diversi negozi di vendita al dettaglio dotate di un sistema informatico obsoleto, dove erano conservati, senza che fossero stati mai cancellati, nomi, indirizzi, numeri di telefono, indirizzi e-mail e cronologia degli acquisti di circa 385 mila clienti.

violazione del principio di limitazione della conservazione di cui all'art. 5, comma 1, lett. e), i dati non erano "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati".

139

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy Greco vs Price Waterhouse business solutions

150 mila euro. per la violazione dell'articolo 5 del Regolamento Ue poiché ai dipendenti della società era stato chiesto di fornire il consenso al trattamento dei loro dati personali, dandogli la falsa impressione che stesse trattando i loro dati secondo la base giuridica del consenso, mentre in realtà i loro dati venivano trattati sotto base giuridica diversa, della quale, tra l'altro, i dipendenti non erano mai stati informati.

Poiché il dipendente si trova in una situazione subordinata e di soggezione rispetto al datore di lavoro, il consenso non può considerarsi «libero» poiché questo non sarebbe tranquillo nel revocare l'eventuale consenso prestato temendone gli effetti.

Oltre alla sanzione pecuniaria, esercitati i poteri correttivi previsti dall'articolo 58, per i quali entro tre mesi, dunque, la società avrebbe dovuto regolarizzare i trattamenti, e di conseguenza le informative, inserendo la corretta base giuridica, che nell'ambito del rapporto di lavoro non è il consenso, ma il contratto individuale o la legge (adempimenti fiscali, previdenziali, contabili o collegati alla sicurezza sul lavoro).

Il Garante greco ha punito la società anche per il fatto di non avere individuato documentazione relativa all'adeguamento privacy.

140

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy italiano vs Casaleggio e associati

50.000 euro con provvedimento n. 83 del 4 aprile 2019 comminati all'Associazione Rousseau, quale responsabile del trattamento per la violazione di cui al combinato disposto degli artt. 32 e 83, paragrafo 4, lettera a) del Regolamento UE 2016/679 oltre ad ingiungere alla stessa associazione i necessari adeguamenti indicati nel Provvedimento.

In precedenza data breach del 2017 con provvedimento del 21 dicembre 2017 in cui si richiedeva riesame delle condizioni di sicurezza e correzione di criticità rilevate.

Ad aprile 2019 pur riconoscendo un sostanziale innalzamento dei livelli di sicurezza dei trattamenti effettuati rileva ancora importanti vulnerabilità che portano alla sanzione.

Rispetto a quanto sancito dall'art. 32 del GDPR ha contestato:

il mancato completo tracciamento degli accessi al database e delle operazioni sullo stesso compiute (violazione del generale dovere di controllo sulla liceità dei trattamenti gravante sul titolare del trattamento e dell'obbligo di assicurare adeguate garanzie di riservatezza agli iscritti in ragione delle dimensioni delle banche dati in questione, e della tipologia di dati raccolti;

la condivisione delle credenziali di autenticazione da parte di più incaricati dotati di elevati privilegi per la gestione della piattaforma e **mancata definizione e configurazione dei differenti profili di autorizzazione** in modo da limitare l'accesso ai soli dati necessari nei diversi ambiti di operatività. (violazione dell'obbligo di predisposizione di misure tecniche e organizzative adeguate).

141

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy italiano vs Casaleggio e associati

Rousseau: Antonello Soro risponde a Davide Casaleggio

Dichiarazione di Antonello Soro, Presidente Garante Privacy

"Con le affermazioni rese a "Povera patria", il signor Casaleggio ripropone una sua rassicurante lettura delle gravi carenze, sotto il profilo della sicurezza informatica, che contrassegnavano la piattaforma "Rousseau" prima dell'intervento del Garante per la Privacy.

Il tentativo di spostare, sul terreno dello scontro politico, un caso di obiettiva e non banale violazione delle leggi (pratica non esattamente nuovissima nello scenario della cronaca italiana), non meriterebbe, di per sé, alcun commento.

L'infondatezza delle accuse di "politicità" mosse all'azione del Garante è così palese che il provvedimento sanzionatorio non è stato impugnato e le sue prescrizioni, ottemperate, sono state espressamente definite utili a "migliorare la piattaforma" dallo stesso Casaleggio.

Valuterò l'opportunità di acquisire la registrazione dell'intervista per tutelare, in sede giudiziaria, i miei diritti e far valere il danno, così determinato, all'immagine dell'Autorità, i cui provvedimenti sono stati sempre improntati al solo obiettivo della corretta applicazione della legge.

Respingo, dunque, queste pretestuose affermazioni, nella ferma consapevolezza dell'indipendenza di giudizio, correttezza assoluta, massima garanzia che hanno sempre contrassegnato l'agire mio e quello del Collegio del Garante, in questi sette anni".

Roma, 11 novembre 2019

142

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy francese vs Carrefour

2.250.000,00 Euro da parte dell'autorità Garante nazionale francese a Carrefour France per diverse violazioni nel trattamento dei dati personali dei propri clienti.

1. Alla luce del gran numero di dati personali di clienti, che acquisiva con le tessere di fidelizzazione, l'informativa fornita rispetto all'acquisizione ed al loro successivo utilizzo, non è stata considerata di facile lettura e poco accessibile in quanto inserita e confusa in altri lunghi documenti.
2. mancanza di informazioni sull'utilizzo dei cookies, che in automatico passavano al dispositivo del cliente connesso, senza richiedere autorizzazione.
3. Mancato rispetto dei tempi di conservazione dei dati, (più di 28 milioni di clienti, inattivi da oltre cinque anni, erano ancora presenti nel database del programma di fidelizzazione. (con durata prevista per quattro anni, da l'ultimo acquisto, ritenuta comunque eccessiva).
4. Per scoraggiare gli interessati ad esercitare il loro diritto di accesso, (art. 12), per esigere sistematicamente un documento di identità, alla persona che cercava di esercitare i propri diritti, non aver risposto a ripetute richieste degli interessati, di accesso piuttosto che di cancellazione.
5. Per la violazione dell'articolo 5 che impone al titolare l'obbligo di trattare in maniera corretta e trasparente i dati degli interessati.

143

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il Garante privacy italiano vs TIM

La sanzione piu alta in Italia - 28.000.000,00 Euro per telemarketing selvaggio che ha pescato da una lista a disposizione di TIM di 50 milioni di numerazioni, con 650 campagne di telemarketing nel periodo luglio 2018-febbraio 2019, indagate dall'Authority

1. Telemarketing selvaggio anche nei confronti di persone iscritte nel registro delle opposizioni o di chi aveva esplicitamente e ripetutamente comunicato di non voler essere disturbato
2. Scarsa vigilanza sui partner che si sono occupati delle campagne promozionali,
3. raccolta del consenso indifferenziata senza possibilità per l'interessato di scegliere
4. conservazione delle informazioni oltre il periodo consentito,
5. gestione dei data breach non idonea

Il Garante si è mosso dopo aver ricevuto negli ultimi due anni centinaia di segnalazioni e reclami e a luglio 2019, dopo le ispezioni presso Tim svolte anche con l'ausilio del nucleo speciale privacy della Guardia di finanza, ha avviato il procedimento che ha portato alla sanzione plurimilionaria.
L'intervento dell'autorità è stato ad ampio raggio (inibitorio, prescrittivo e sanzionatorio) «in grave difformità» alle norme sulla privacy, per un fenomeno che, nonostante gli interventi del legislatore e del Garante, non si è per nulla attenuato, portando ai 27,8 milioni della sanzione amministrativa, anche per via della recidiva e dei simili comportamenti che già avevano indotto il Garante ad intervenire nei confronti di TIM, e che l'operazione contetstata aveva portato notevolivantaggi economici alla società.

144

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DOTT. FRANCESCO FARINA

Università degli Studi di Roma Tor Vergata

francesco.farina@uniroma2.it

145