FONDAZIONE ENI ENRICO MATTEI

La normativa privacy in FEEM

Giancarlo Butti

FEEM
Milano

La normativa

Dlgs 196/03

Allegati A1-A6, B, C

Atti del Garante per la protezione dei dati personali:

- **Provvedimenti**
- **Linee guida**
- **Autorizzazioni**

675/96 (abrogata)

Dpr 318/99 (abrogata)

Normative collegate

Costituzione

Statuto dei lavoratori

518/92 ..

248/00 “Protezione software e banche dati”

547/93 “Computer crime”

626/94 “Sicurezza”

Adempimenti previsti

Burocratici

Organizzativi

Tecnologici

Adempimenti

Burocratici

- **Notifica**
- **Autorizzazioni**
- **Informative**
- **Consenso**

Organizzativi

- **Designazioni**
- **Incarichi**

Tecnici

- **Misure di sicurezza minime e adeguate**
- **Sicurezza fisica**

Chi è coinvolto

Aziende

Professionisti

Enti pubblici

Enti non profit

In misura minore anche il privato cittadino

Cosa tutela

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

Definizioni

Dato personale

Dato sensibile

Dato giudiziario

Trattamenti che presentano rischi specifici

Dato personale

b) "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Esempi di dati personali:

Nome, indirizzo, immagine, voce, targa dell'auto…

Dato sensibile

d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Esempi di dati personali sensibili:

Assenze dal lavoro, trattenute sindacali, log di navigazione internet…

Dato giudiziario

e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Trattamento che presenta rischi specifici

Art. 17. Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

Trattamento

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

Modalità di trattamento

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati

Cosa non tutela

I dati anonimi

n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

I dati statistici

I dati riservati (se non anche personali)

Le figure coinvolte

Chi tratta i dati

- **Titolare**
- **Rappresentante nello stato**

- **Responsabile**
- **Incaricato**

I soggetti di cui si trattano i dati

- **Interessato**

Titolare

Art. 28. Titolare del trattamento

1. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Responsabile

Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Incaricato

Art. 30. Incaricati del trattamento

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Interessato

i) "interessato", la persona fisica cui si riferiscono i dati personali: (2)

La nomina del responsabile

Il responsabile può essere:

- **interno**
- **esterno**

- **persona fisica**
- **persona giuridica**

La nomina è un contratto

Il responsabile può rifiutare la nomina

La lettera di incarico

L’incaricato è:

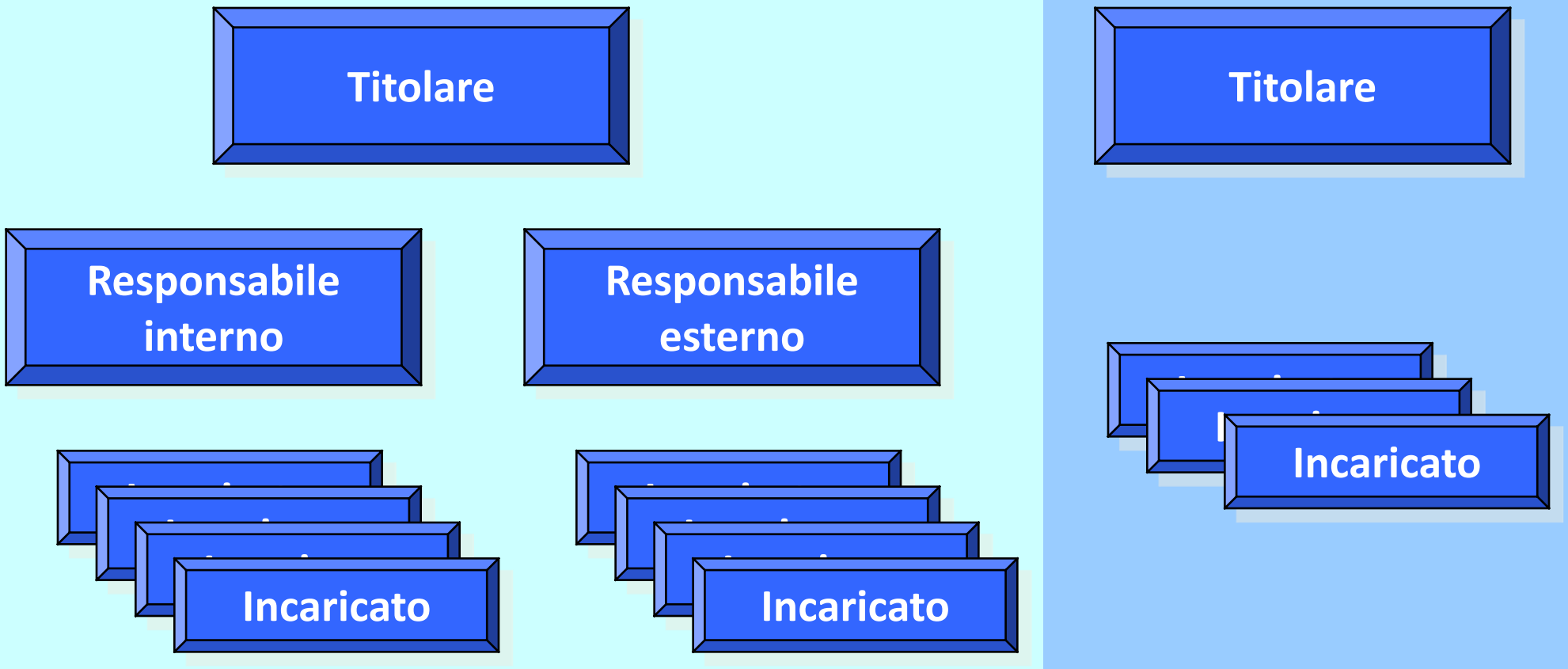
- **interno**
- **esterno**

- **solo persona fisica**

L’incarico autorizza a trattare i dati

Senza lettera di incarico non è possibile trattare i dati

Le relazioni fra le figure



Le implicazioni delle relazioni

Fra Titolare e Responsabile

Fra Titolare ed Incaricato

Fra Responsabile ed Incaricato

non vi è comunicazione dei dati

Fra Titolare e Titolare

vi è comunicazione di dati

La comunicazione richiede in genere il consenso dell'interessato

Le implicazioni delle relazioni

La nomina a Responsabile è specifica

La nomina può essere reciproca relativamente a trattamenti diversi

Non possono esistere catene di responsabilità

Gli adempimenti burocratici

Notifica

Autorizzazioni

Informativa

Consenso

Notifica

Art. 37. Notificazione del trattamento

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;

b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;

c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;

Notifica

d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;

e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;

f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

1-bis. La notificazione relativa al trattamento dei dati di cui al comma 1 non è dovuta se relativa all'attività dei medici di famiglia e dei pediatri di libera scelta, in quanto tale funzione è tipica del loro rapporto professionale con il Servizio sanitario nazionale.

Notifica

Quando va effettuata

Prima di iniziare il trattamento

Come viene effettuata

Solo per via telematica

Autorizzazioni

Chi deve farla

Titolare che tratta dati sensibili

Quando va effettuata

Prima di iniziare il trattamento

Come viene effettuata

Comunicazione al Garante

Autorizzazioni generali

Autorizzazione generale n. 1/2014 al trattamento dei dati sensibili nei rapporti di lavoro

Autorizzazione generale n. 2/2014 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale

Autorizzazione generale n. 3/2014 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni

Autorizzazione generale n. 4/2014 al trattamento dei dati sensibili da parte dei liberi professionisti

Autorizzazione generale n. 5/2014 al trattamento dei dati sensibili da parte di diverse categorie di titolari

Autorizzazione generale n. 6/2014 al trattamento dei dati sensibili da parte degli investigatori privati

Autorizzazione generale n. 7/2014 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici

Autorizzazione generale n. 8/2014 al trattamento dei dati genetici

Autorizzazione generale n. 9/2014 al trattamento dei dati personali effettuato per scopi di ricerca scientifica

Informativa

Quando va effettuata

- **Prima di iniziare il trattamento**
- **All'interessato**
- **Al soggetto presso il quale si recuperano i dati**

In che forma

- **Orale**
- **Scritta**

Modalità di documentazione

- **Consigliabile scritta**

Informativa

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

Consenso

Quando va effettuata

- **Dopo aver rilasciato l'informativa**

In che forma

- **Documentato per iscritto**
- **Sottoscritto (dati sensibili)**

Modalità di documentazione

- **Consigliabile sottoscritto**

Casi di esclusione

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

Casi di esclusione

e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei princìpi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

Casi di esclusione

h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;

Casi di esclusione

i-bis) riguarda dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis; (2)

i-ter)con esclusione della diffusione e fatto salvo quanto previsto dall'articolo 130 del presente codice, riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'articolo 2359 del codice civile ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrativo contabili, come definite all'articolo 34, comma 1-ter, e purché queste finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13.

Problemi

Rilascio dell'informativa

- **Difficoltà oggettive nel rispettare la normativa**

Richiesta di consenso

- **I casi di esclusione possono essere vanificati**

Gestione del consenso

La gestione nel tempo del consenso

- **il consenso è specifico**
- **riguarda alcuni trattamenti**
- **può essere revocato da parte dell'interessato**

Non si può dar luogo ad un nuovo trattamento su dati già raccolti senza aver rilasciato apposita informativa ed eventuale consenso

I diritti dell’interessato

Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

I diritti dell'interessato

3. L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale

La gestione dei diritti

L’interessato può far valere i suoi diritti:

- **senza formalità**
- **con richieste anche in forma orale**
- **rivolgendosi a qualunque incaricato**

L’azienda deve essere pronta a rispondere in tempi brevissimi ad ogni richiesta

Le implicazioni

L’azienda deve avere sotto controllo tutto il proprio patrimonio informativo, sia esso in formato elettronico o cartaceo

Gli incaricati devono essere adeguatamente informati e formati per rispondere alle richieste degli interessati

Il trasferimento di dati all'estero

Distinguere fra

- **Persona fisica**
- **Persona giuridica**

Stato dove viene trasferito

- **UE**
- **Extra UE**

La responsabilità civile

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11

Le misure di sicurezza

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

Le misure di sicurezza

Misure minime

L'adozione delle misure minime permette al Titolare il rispetto della normativa evitando un illecito penale

Misure adeguate

L'adozione delle misure adeguate (superiori a quelle minime prescritte dalla normativa) permette al Titolare di tutelarsi (in parte) rispetto alla responsabilità civile

DPS (Documento programmatico sulla sicurezza)

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Abrogato

DPS

Il DPS costituisce una misura adeguata, quindi anche se è stato abrogato come misura minima è opportuno redigere un documento che ne ricalchi i contenuti pur non essendoci un obbligo ed una scadenza

Principali misure di sicurezza

- **Sistema di autenticazione informatica**
- **Sistema di autorizzazione**
- **Verifica periodica delle autorizzazioni**
- **Sistemi antivirus e codice malevolo**
- **Gestione delle vulnerabilità ed aggiornamento periodico**
- **Backup periodico**
- **Redazione DPS**
- **Sistemi anti intrusione**
- **Gestione dei supporti**
- **Capacità di ripristino**
- **Certificazione degli interventi di terzi**
- **Dichiarazione in sede di bilancio**
- **Gestione archivi cartacei**

Le sanzioni

Le violazioni amministrativi si hanno nei seguenti casi:

- **Omessa o inidonea informativa all'interessato**
- **Cessione di dati**
- **Comunicazione di dati personali idonei a rilevare lo stato di salute**
- **Omessa o incompleta notificazione**
- **Omessa informazione o esibizione al Garante**

Le sanzioni

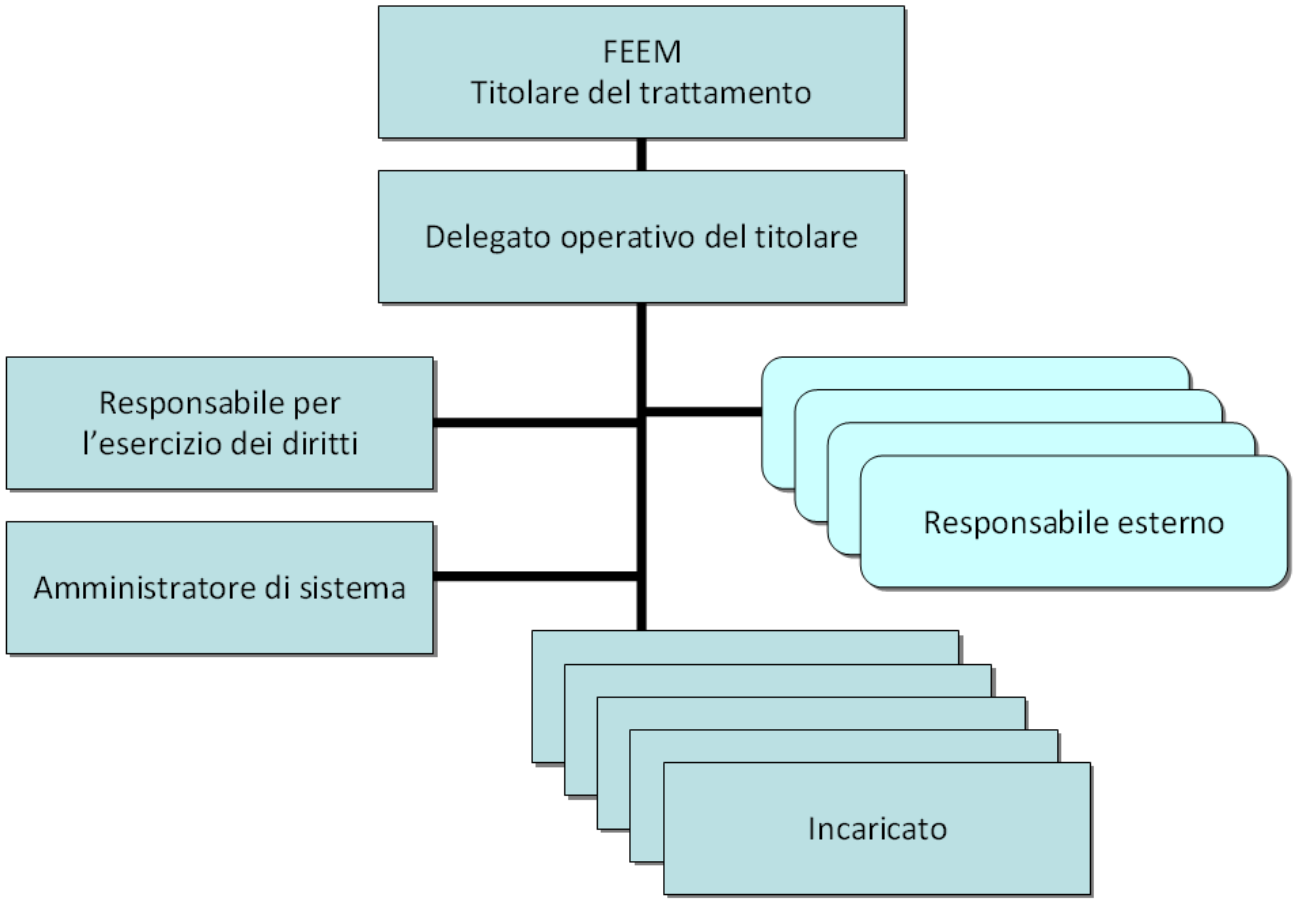
Gli illeciti penali si hanno nei seguenti casi:

- **Trattamento illecito di dati**
- **Falsità nelle dichiarazioni e notificazioni al Garante**
- **Mancata adozione delle misure di sicurezza**
- **Inosservanza di provvedimenti del Garante**

L’organizzazione privacy in FEEM

Titolare del trattamento	**FEEM**
Delegato dal Titolare	**Direttore generale pro tempore**
Responsabile interno del trattamento ai fini dell’esercizio dei diritti degli interessati	**Direttore generale pro tempore**
Struttura alla quale è demandato il compito di coordinamento e supervisione nell’ambito della normativa privacy	**Servizi Generali**
Struttura alla quale è demandato il compito di curare l’implementazione delle misure di sicurezza dal punto di vista informatico	**Servizi ICT**
Soggetti tenuti al rispetto della normativa privacy e del presente Regolamento	**Tutti gli incaricati di FEEM, indipendentemente dal tipo di rapporto contrattuale, anche temporaneo, in essere.**

L’organizzazione privacy in FEEM



Modello per segnalare eventi con impatti privacy

Modello per la segnalazione DO01

Ufficio segnalante	
Data segnalazione	

Nuovi rapporti/Variazioni con soggetti esterni	
	Nuove tipologie di interessati
	Soggetti esterni che svolgono attività per conto della Fondazione
	Soggetti esterni per i quali la Fondazione svolge delle attività
	Soggetti esterni che svolgono attività congiuntamente alla Fondazione
Variazione nei servizi acquisiti/forniti	
	Nuovi servizi acquisiti
	Nuovi servizi forniti
	Variazioni nella modalità con cui viene effettuato un servizio
Variazioni organizzative/tecnologiche/logistiche	
	Variazione nei processi
	Variazioni nel sistema informativo
	Variazioni organizzative
	Variazioni del personale
	Variazione nei fornitori
	Variazioni nella logistica

Descrizione della variazione prevista

Elementi da rilevare

ELEMENTI CHE POSSONO AVERE IMPATTI SUGLI ADEMPIMENTI PRIVACY	
Elemento primario	**Elemento secondario**
Nuovi rapporti/ Variazioni con soggetti esterni	
	Nuove tipologie di interessati
	Soggetti esterni che svolgono attività per conto della Fondazione
	Soggetti esterni per i quali la Fondazione svolge delle attività
	Soggetti esterni che svolgono attività congiuntamente alla Fondazione
Variazione nei servizi acquisiti/forniti	
	Nuovi servizi acquisiti
	Nuovi servizi forniti
	Variazioni nella modalità con cui viene effettuato un servizio
Variazioni organizzative/tecnologiche/logistiche	
	Variazione nei processi
	Variazioni nel sistema informativo
	Variazioni organizzative
	Variazioni del personale
	Variazione nei fornitori
	Variazione nella logistica

Elementi da rilevare

Azione da compiere
Nel caso in cui sia previsto uno degli eventi sopra elencati deve essere data preventiva comunicazione all'Ufficio Servizi Generali al fine di valutare gli impatti in ambito privacy mediante l'apposito modello DO01 disponibile nella intranet aziendale
Possibili impatti
Rilascio di lettere di incarico
Definizione di ruoli privacy – clausole contrattuali
Predisposizione e rilascio di informative
Richiesta e gestione del consenso
Definizione misure di sicurezza
Implementazione misure di sicurezza
Verifica misure di sicurezza
Notifica
Verifica di autorizzazioni
Accordi sindacali

Procedure in ambito privacy in FEEM

DIFFUSIONE DI DATI PERSONALI

La Fondazione diffonde dati personali, in particolare relativi ai propri collaboratori:

- sui propri siti e blog
- attraverso pubblicazioni di libri e riviste
- attraverso social network
- attraverso le proprie newsletter
- nel corso di eventi e convegni.

Le informazioni diffuse possono riguardare:

- dati anagrafici
- immagini
- filmati (anche tramite youtube)

La diffusione di tali dati richiede una preventiva specifica autorizzazione da parte degli interessati.

Canale di diffusione	Attività e procedura da adottare
Nuovo sito o nuovi servizi su siti esistenti che comportano diffusione di dati personali	Verifica che i soggetti i cui dati saranno diffusi: • siano stati adeguatamente informati sulla tipologia di dati diffusi e sullo strumento utilizzato • abbiano rilasciato specifico consenso Inserire specifica indicazione nelle informative. Inserire specifica richiesta di consenso aggiuntiva alle altre.
Pubblicazioni di articoli o libri, newsletter, sia in formato cartaceo, che elettronico	
Presentazione durante eventi	

Procedure in ambito privacy in FEEM

GESTIONE DI LISTE ed INVITO A EVENTI

La Fondazione dispone, in proprio o per conto di terzi, di un rilevante numero di dati relativi a persone fisiche, ivi compreso l'indirizzo di posta elettronica.

Tali dati sono utilizzati per l'inoltro di newsletter, inviti ad eventi...

La gestione di tali database non è centralizzata, ma parcellizzata.
Lo stesso nominativo può apparire in più liste.

La materia specifica è regolata da vari articoli del Dlgs 196/03, oltre che da

- *Linee guida in materia di attività promozionale e contrasto allo spam - 4 luglio 2013*
- *Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto - 15 maggio 2013*

Uso delle liste	Attività e procedura da adottare
Invito ad eventi	Verifica che i soggetti abbiano rilasciato specifico consenso. Inserire specifica indicazione nelle informative. Inserire specifica richiesta di consenso aggiuntiva alle altre. Inserire la possibilità di richiedere l'interruzione dell'inoltro delle comunicazioni con modalità automatizzata.
Inoltro newsletter	

Procedure in ambito privacy in FEEM

GESTIONE EVENTI

Durante lo svolgimento degli eventi organizzati da FEEM possono essere trattati i dati dei partecipanti nel caso in cui:

- la partecipazione all'evento comporti una specifica registrazione del soggetto interessato
- l'evento venga ripreso mediante registrazioni audio e video (al riguardo si vedano anche le regole per la diffusione dei dati personali).

Nel caso in cui l'evento si svolga presso i locali della Fondazione, valgono anche gli altri trattamenti in essere per gli ospiti:

- videosorveglianza
- registrazione dell'accesso

per i quali sono già in essere gli opportuni presidi.

Registrazione	Attività e procedura da adottare
Registrazione specifica all'evento	Rilascio di specifica informativa La richiesta o meno del consenso è legata al tipo di dati raccolti ed al loro successivo utilizzo, in particolare per quanto attiene il successivo riutilizzo per informare il soggetto interessato su nuove iniziative della Fondazione
Registrazione audio video dell'evento	Rilascio di specifica informativa Richiesta di consenso per la ripresa audio e video Nel caso in cui il video debba essere successivamente diffuso, richiesta di specifico consenso per questa finalità La presenza del consenso è condizionante alla partecipazione all'evento del soggetto interessato essendo di fatto impossibile effettuare riprese selettive salvo predisporre specifiche aree non riprese

Procedure in ambito privacy in FEEM

CREAZIONE NUOVI SITI O NUOVI SERVIZI (cookies e profilazione)

L'attività di creazione di nuovi siti della Fondazione o di terzi per i quali la Fondazione svolge attività comporta:

- un trattamento dei dati personali degli utenti dei siti
- un possibile trattamento di ulteriori dati personali nel caso siano attivati servizi quali ad esempio:
  - modulo di richiesta informazioni
  - modulo di iscrizione a newsletter o altri servizi
  - contatti che consentano l'inoltro di comunicazioni
  - ...

La policy della Fondazione in merito all'uso di cookies prevede:

- non sono utilizzati cookies diversi da quelli tecnici
- possono essere utilizzati da terze parti cookies

La policy della Fondazione in merito alla profilazione degli utenti dei siti prevede:

- non vengono effettuate profilazioni degli utenti

Attività preliminari

Attività preliminari	Attività e procedura da adottare
Verifica titolare	Individuare il titolare del sito
Policy privacy	Pubblicazione della policy privacy base
Cookies	Verificare se i servizi abilitati sul sito utilizzino cookies e redigere la relativa informativa
Profilazione	Verificare se i servizi ai quali accedono gli utenti effettuino una profilazione degli utenti
	Compilare il modulo riepilogativo

Procedure in ambito privacy in FEEM

SOCIAL NETWORK

La Fondazione dispone di proprie pagine sui principali social network:

- Linkedin
- Facebook
- Twitter

Dal punto di vista normativo la materia è regolata dal Provvedimento del Garante per la protezione dei dati personali ***Linee guida in materia di attività promozionale e contrasto allo spam - 4 luglio 2013.***

Tipo di canale	Attività e procedura da adottare
Linkedin Facebook Twitter	Nel caso in cui si desiderino utilizzare in modo attivo i contatti di un canale predisporre nella pagina principale adeguata informativa che indichi tale possibilità prima dell'adesione.

xnel caso in cui un utente sia diventato "fan" della pagina di una determinata impresa o società oppure si sia iscritto a un "gruppo" di follower di un determinato marchio, personaggio, prodotto o servizio (decidendo così di "seguirne" le relative vicende, novità o commenti) e successivamente riceva messaggi pubblicitari concernenti i suddetti elementi… l'invio di comunicazione promozionale riguardante un determinato marchio, prodotto o servizio, effettuato dall'impresa a cui fa riferimento la relativa pagina, può considerarsi lecita se dal contesto o dalle modalità di funzionamento del social network, anche sulla base delle informazioni fornite, può evincersi in modo inequivocabile che l'interessato abbia in tal modo voluto manifestare anche la volontà di fornire il proprio consenso alla ricezione di messaggi promozionali da parte di quella determinata impresa.

Se invece l'interessato si cancella dal gruppo, oppure smette di "seguire" quel marchio o quel personaggio, o comunque si oppone ad eventuali ulteriori comunicazioni promozionali, il successivo invio di messaggi promozionali sarà illecito, con le relative conseguenze sanzionatorie.

Ciò, ferma comunque restando la possibilità, talora fornita dai social network ai loro utenti, di bloccare l'invio di messaggi da parte di un determinato "contatto" o di segnalare quest'ultimo come spammer.

Nell'ipotesi dei "contatti" (i c.d. "amici") dell'utente, dei quali spesso nei social network o nelle comunità degli iscritti ai servizi di cui sopra, sono visualizzabili numeri di telefono o indirizzi di posta elettronica, l'impresa o società che intenda inviare legittimamente messaggi promozionali dovrà aver previamente acquisito, per ciascun "contatto" o "amico", un consenso specifico per l'attività promozionale.

Procedure in ambito privacy in FEEM

CONDIVISIONE CLOUD

La componenti della normativa privacy che regolano l'utilizzo dei servizi cloud riguardano gli aspetti di:

- sicurezza
- definizione dei ruoli privacy
- trasferimento dati all'estero

Tipo di canale	Attività e procedura da adottare
Dropbox	Regolamentato nelle Norme di comportamento

Il nuovo Regolamento privacy EU

Entrata in vigore

Articolo 91 ***Entrata in vigore e applicazione***

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

2. Esso si applica a decorrere da [*due anni dalla data di cui al paragrafo 1*].

Il Regolamento UE è immediatamente operativo in tutti gli Stati UE e non ha bisogno di recepimento nelle normative nazionali.

La normativa comunitaria è prioritaria in caso di difformità da quella nazionale.

Tutti i provvedimenti dell'autorità Garante restano in vigore per la parte coerente con il nuovo Regolamento UE.

Principi fondamentali

Applicazione della norma anche fuori dall'UE

Protezione fin dalla progettazione e protezione di default

Valutazione d'impatto sulla protezione dei dati e analisi dei rischi

Accountability di chi effettua il trattamento

Documentazione dettagliata dei trattamenti e delle misure di sicurezza

Corresponsabilità dei vari attori coinvolti nel trattamento

Obbligo di notifica delle violazioni all'autorità ed agli interessati

Consenso esplicito da parte dell'interessato

Diritto all'oblio ed alla cancellazione

Diritto alla portabilità dei dati

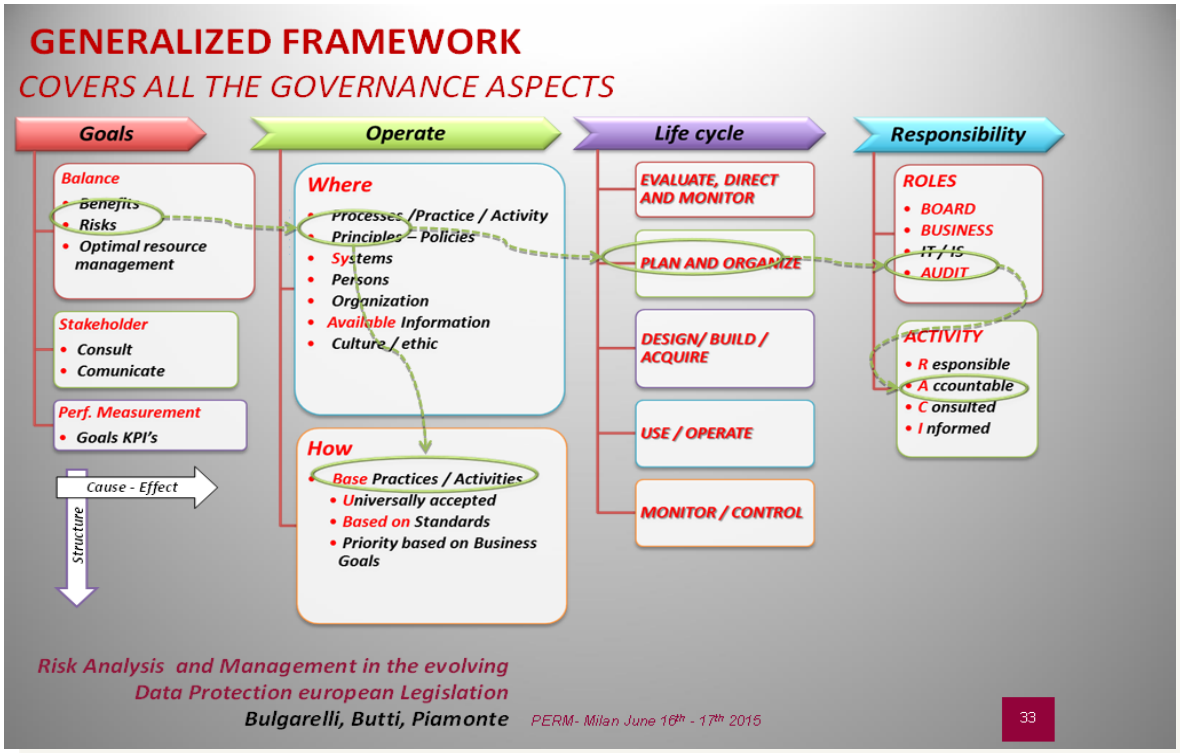
Designazione del responsabile della protezione dei dati

Regole per il trasferimento dati a terzi

Aumento notevole delle sanzioni

Codici di condotta e certificazione

Accountability e documentazione



Security

by **Direttiva**

Compliance

Compliance

by **Regolamento**

Security

Chi effettua il trattamento deve dimostrare di rispettare la normativa; si passa da **SOSTANZA** a **FORMA**.

Non esistono check list o regole definite; è quindi opportuno riferirsi a framework e standard consolidati

FONDAZIONE ENI ENRICO MATTEI

Responsabile della protezione dei dati: i compiti

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) **informare e consigliare** il responsabile del trattamento o l'incaricato del trattamento nonché i *dipendenti* che trattano dati personali in merito agli **obblighi** derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla **protezione dei dati**;

b) **sorvegliare l'osservanza** del **presente regolamento**, delle **altre disposizioni** dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle **politiche** del responsabile del trattamento o dell'incaricato del trattamento in materia di protezione dei dati personali, compresi **l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale** che partecipa ai trattamenti e gli **audit connessi**;

…

f) fornire, se richiesto, un **parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento** ai sensi dell'articolo 33;

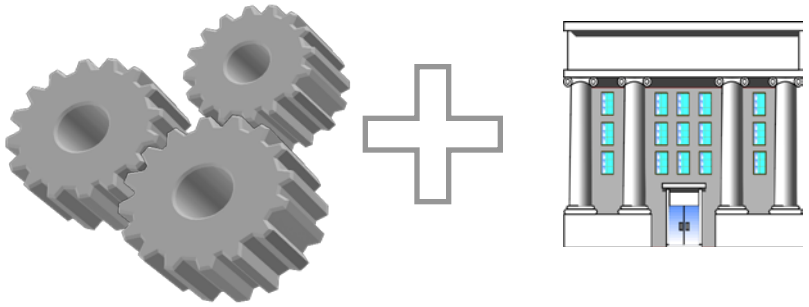
g) **cooperare con l'autorità di controllo**;

h) fungere da **punto di contatto per l'autorità di controllo** per questioni connesse al trattamento di dati personali, tra cui la **consultazione preventiva** di cui all'articolo 34, ed effettuare, se del caso, **consultazioni su qualunque altra questione**.

2. (…)

2 bis. Nell'eseguire i propri compiti il responsabile della protezione dei dati **considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del medesimo.**

Privacy by design



Oggi il coinvolgimento degli aspetti privacy avviene (se avviene…) alla conclusione della progettazione/realizzazione di un prodotto/servizio e riguarda in genere solo aspetti formali (informative, clausole contrattuali…)

Data Oriented Strategies

Minimise

Hide

Separate

Aggregate

Process Oriented Strategies

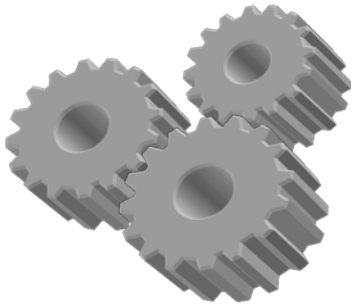
Inform

Control

Enforce

Demonstrate

Con il nuovo Regolamento UE la valutazione degli impatti privacy (PIA) e la valutazione degli interventi tecnici (oltre che organizzativi e formali) deve avvenire dalla fase di progettazione



Notifica di violazione

Tipo di violazione

Lettura (presumibilmente i dati non sono stati copiati)

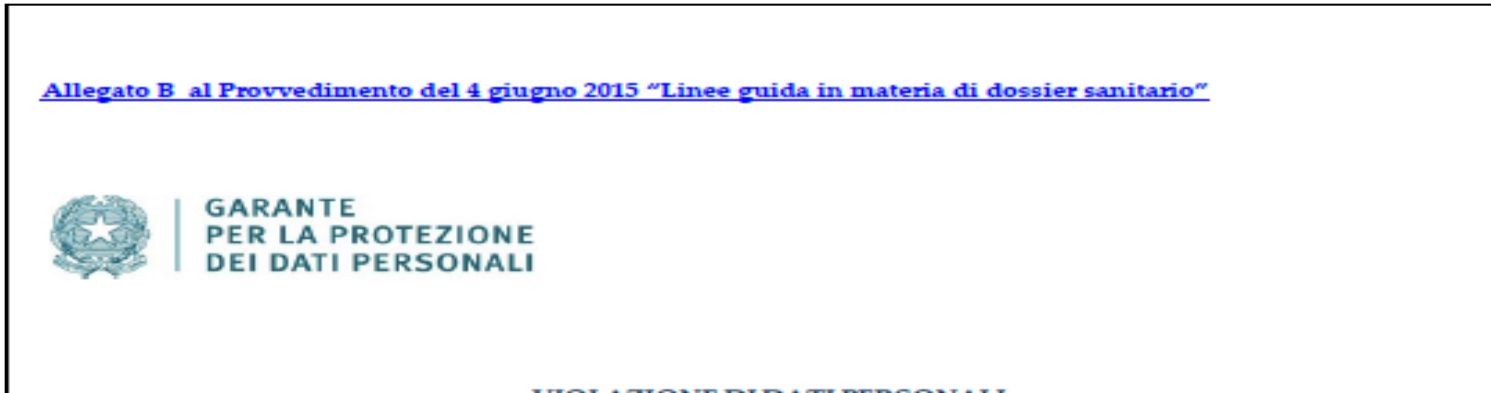
Copia (i dati sono ancora presenti sui sistemi del titolare)

Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

Altro:


Allegato B al Provvedimento del 4 giugno 2015 "Linee guida in materia di dossier sanitario"

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Sanzioni massime

In conformità del paragrafo 2 bis, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a **20 000 000** EUR, o per le imprese, fino al **4**% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

Contatti: giancarlo.butti@feem.it