CERTIFICAZIONE - GDPR
ISDP 10003:2015

DATA PROTECTION CERTIFIED
ISDP 10003:2015

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO
PRD N° 189 B
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
Signatory of EA, IAF and ILAC Mutual Recognition Agreements

DIRITTO AL RISARCIMENTO E SANZIONI

Ogni Autorità di Controllo garantisce che le sanzioni amministrative pecuniarie comminate in relazione alle violazioni del Regolamento siano:

«EFFETTIVE, PROPORZIONATE E DISSUASIVE»

DIRITTO AL RISARCIMENTO E SANZIONI

La violazione di cui agli artt: 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 e 43

È punita con sanzione amministrativa pecuniaria fino a **10.000.000** euro o fino al **2%** del fatturato mondiale annuo.

La violazione di cui agli artt: 5, 6, 7 e 9; da 12 a 22 da 44 a 49.

È punita con sanzione amministrativa pecuniaria fino a **20.000.000** euro o fino al **4%** del fatturato mondiale annuo.

VIOLAZIONE	SANZIONE AMMINISTRATIVA	SANZIONE PENALE
OMESSA O INIDONEA INFORMATIVA	ART. 161 **6.000€ - 36.000€** **(ovvero 2.400€ - 2.400.000€)**	
CESSIONE NON AUTORIZZATA DATI PERSONALI	ART 162 COMMA 1 **4.000€ - 2.400.000€**	ART. 167 **6 MESI – 3 ANNI RECL**
TRATTAMENTO ILLECITO DI DATI (ARTT. 18,19, 23, 123, 126, 130)	ART. 162 COMMA 2 BIS **10.000€ - 2.400.000€**	ART. 167 **6 MESI – 18 MESI** SE IL FATTO CONSISTE NELLA COMUNICAZIONE O DIFFUSIONE **6 MESI -24 MESI RECL** Art.167 COMMA 2 **1 ANNO – 3 ANNI**
OMESSA O INCOMPLETA NOTIFICAZIONE AL GARANTE	ART. 163 **8.000€ - 2.400.000€**	
MANCATA ADOZIONE MISURE MINIME DI SICUREZZA	ART. 162 COMMA 2 BIS **10.000€ - 2.400.000€**	ART.169 **ARRESTO FINO A 2 ANNI** (POSSIBILE OBLAZIONE ENTRO 6 MESI)
INOSSERVANZA DEI PROVVEDIMENTI DEL GARANTE		ART.170 **6 MESI – 3 ANNI RECL**

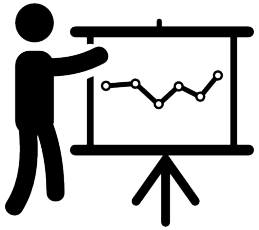
Esempi?

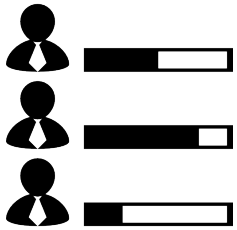
E’ uno schema di **certificazione volontario**, accreditato da ACCREDIA, per determinare la conformita’ al GDPR.

Fornisce i principi e gli elementi di controllo (Annex) per una completa valutazione della conformità dei processi interni all’organizzazione in merito alla protezione dei dati personali con particolare riferimento alla corretta gestione dei rischi.

Cosa è ISDP?

- lo schema ISDP 10003:2015 **è applicabile a tutte le tipologie di organizzazioni** e specifica i requisiti per la gestione in correttezza, sicurezza e conformità delle persone fisiche con particolare riguardo ai dati personali (*art. 1 paragrafo 1*).





A chi si rivolge

- Il Nuovo Regolamento europeo ha cambiato lo scenario delle imprese pubbliche e private che operano nell'ambito della gestione della data protection!

COME?

Con un approccio sostanziale…

Il contesto…

GDPR cosa cambia

GDPR rivoluzione culturale

TITOLARE

d.lgs. 196/03

Concetto formale

- Nomine
- Misure **minime**
- DPS

EU Reg. 2016/679

Concetto sostanziale

- Accountability
- Misure **adeguate**
- Aggiornamento TEMPESTIVO dei dati
- Valutazione del rischio
- Valutazione d'impatto
- Privacy by design e by default

★**4 STEP** PER COMPRENDERE LA CENTRALITA' DEL SISTEMA DI CERTIFICAZIONE

Art. 5 - Principi del Trattamento dei Dati Personali

Art. 24 - Responsabilità del Titolare

Art. 42 – Meccanismi di certificazione

Art. 43 – Organismi di certificazione

ISDP nel Regolamento EU

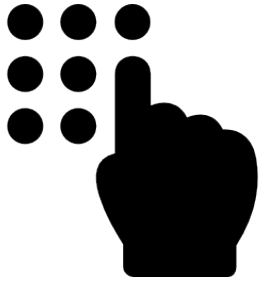
STEP 1

Art. 5

I principi del trattamento dei dati personali

Paragrafo. I

a) Liceità, correttezza e trasparenza
b) Finalità determinate, esplicite e legittime
c) Pertinenti alle finalità
d) Esatti e, se necessario, aggiornati/cancellati
e) Conservati per il tempo della finalità



ART.5

I principi del trattamento dei dati personali

Chi è competente del rispetto del paragrafo 1?

Il Titolare del Trattamento!

Art. 5.I dati personali oggetto di trattamento sono…

…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 e AGGIORNAMENTO

Comma 2

- Il Titolare del trattamento è **competente** per il rispetto del paragrafo 1 e in grado di **comprovarlo**

«Responsabilità»

ACCOUNTABILITY

La violazione di cui agli artt: 5, 6, 7 e 9

- I diritti art. 12 a 22
- I trasferimenti di dati personali a un paese terzo da 44 a 49
- l'inosservanza ai sensi dell'art. 58 com. 2

È punita con sanzione amministrativa pecuniaria fino a **20.000.000** euro o fino al **4%** del fatturato mondiale annuo.

STEP 2

Art. 24

Responsabilità del Titolare

RESPONSABILITA' DEL TITOLARE
FORMAZIONE E CONSAPEVOLEZZA

Con il D.L. 5/2012 con la reg. 19 dell'all. B, è stata eliminata la formazione quale elemento obbligatorio.

Art. 29 – Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare 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.

Art. 32 comma 4) - Il titolare e il responsabile del trattamento fanno si che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'unione o degli stati membri.

Regole per il titolare

Consapevolezza	Accertarsi che le persone interne dell'organizzazione siano consapevoli dell'impatto, mappare le aree di rischio, individuare quelle maggiormente interessate dai cambiamenti e ruoli decisionali. Introdurre nuovi documenti e nuove figure, formazione.
Dati trattati	Documentare i dati personali trattati, da dove arrivano e con chi vengono condivisi. Organizzare procedure di verifica dei dati
Informative	Rivedere le informative e pianificare le modifiche necessarie prima della completa applicazione del regolamento
Diritti dell'interessato	Controllare le proprie procedure in modo da assicurarsi che coprano tutti i diritti degli interessati, compresa la cancellazione e la possibilità di fornire i dati in un formato elettronico di uso comune. (compresa la protabilità e il diritto all'oblio)
Istanze di accesso da parte dell'interessato	Aggiornare le proprie procedure in modo da poter riscontrare le istanze nei tempi previsti, valutare le ipotesi e adottare policy e procedure che consentano di giustificare un eventuale diniego.

Regole per il titolare

Consenso	Rivedere in quali casi e con quali modalità vengono richiesti, ottenuti e registrati i consensi, in che modo da valutare se sia necessario operare modifiche. *(**cons. 171 eu GDPR** - "Qualora il trattamento si basi sul consenso a norma della DIR 95/46/CE, non occorre che l'interessato presti nuovamente il consenso)*
Minori	Valutare la predisposizione di sistemi che consentano la verifica dell'identità dei minori e garantiscano l'acquisizione del consenso da parte del "Titolare della responsabilità genitoriale"
Data breaches	Accertarsi di avere procedure efficaci che consentano di individuare, documentare, investigare e (se necessario) comunicare, come per legge, le violazioni di dati personali.
Protezione dei dati sin dalla progettazione e valutazione d'impatto sulla protezione dei dati	Prendere confidenza con le valutazioni d'impatto sulla protezione dei dati come prima cosa, presuppone aver effettuato una perfetta valutazione dei rischi. Seguire le indicazioni di volta in volta fornite dal gruppo WP 29
Data Protection Officer	Valutare se si rientra nei casi previsti per la designazione del DPO al fine di dimostrare la conformità ai requisiti di sicurezza previsti. Valutare come questo ruolo possa collocarsi in rapporto alla propria struttura considerando le necessarie modifiche anche in ordine alla governance.

Regole per il titolare

Trattamenti transfrontalieri	Verificare se l'organizzazione opera in più stati e se ha più stabilimenti occorrerà mappare i nodi decisionali per determinare sotto quale Autorità si ricade
Accountability	Familiarizzare con i principi di responsabilizzazione e verificare costantemente all'interno dell'azienda il rispetto delle procedure rilasciate.

STEP 3

Art. 42

Certificazione

1) Gli Stati Membri, le Autorità di Controllo, il comitato e la commissione incoraggiano l'istituzione di **meccanismi di certificazione** nonché di **sigilli e marchi** allo scopo di dimostrare la conformità al regolamento

- ✓ **CHI NE GIOVA?** Titolare e Responsabile del Trattamento
- ✓ **DESTINATARI?** Micro, piccole e medie imprese
- ✓ **FORMA:** Volontaria, accessibile
- ✓ **PERIODO DURATA:** max 3 anni

ART.42
Certificazione

STEP 4

Art. 43

Organismi di Certificazione

FEATURES:

- Rilasciano/rinnovano la certificazione e **informano** le autorità di controllo al fine di consentire alle stesse di esercitare i propri poteri
- **Trasmettono** alle autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta (comma 5)
- Devono essere in possesso del livello adeguato di competenze in termini di protezione dei dati
- Devono essere **accreditati** dalle: a) autorità di controllo b) EN ISO/IEC 17065
- Devono aver dimostrato di essere **indipendenti** e **competenti** riguardo al contenuto della certificazione
- No conflitti d'interesse

ART.43

Organismi di Certificazione

Cos'è l'accreditamento?

"**Attestazione** da parte di un organismo nazionale di accreditamento (AB) che **certifica** che un determinato **organismo di valutazione di conformità** (CaB) soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, **compresi quelli definiti nei rilevanti programmi settoriali**, per svolgere una specifica attività di Valutazione della conformità"

Reg. CE n.765/2008

Accreditamento - Reg. 765/2008

REGOLAMENTO EUROPEO EU-GDPR 2016/679

1995

Direttiva 95/46/CE

1996

L. 675/96

2003

D.Lgs 196/2003

2016

Eu GDPR 2016/679

REGOLAMENTO EUROPEO EU-GDPR 2016/679

"Ai titolari del trattamento del settore pubblico e privato sarà richiesto non semplicemente di rispettare le norme, e quindi di fare una check list degli adempimenti minimi, ma di tradurre in pratica questi principi con diversi compiti a casa, in chiave di creatività e proattività.

Dovranno dimostrare di aver distribuito responsabilità al proprio interno, di avere una risposta per i vari problemi, di aver valutato i rischi e le possibili conseguenze e di avere quindi una strategia articolata e trasparente nei confronti dei soggetti cui si riferiscono le informazioni.

Non sarà più una materia delegabile a un funzionario di turno, a un esperto di tecnologia o a un ufficio legale, sarà l'approccio globale che avrà importanza, anche perché si dovranno individuare linee di bilancio importanti"

Dr. Giovanni BUTTARELLI
Presidente Autorità Garante Europea

PRINCIPI GENERALI DEL TRATTAMENTO

ART. 5

- ★ Lecito, equo e trasparente
- ★ Limitazione della Finalità
- ★ Minimizzazione
- ★ Esattezza e aggiornamento
- ★ Limitazione della conservazione

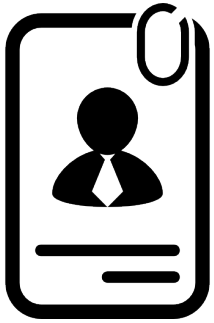
PRINCIPI GENERALI DEL TRATTAMENTO

Art. 5. I DATI PERSONALI OGGETTO DI TRATTAMENTO SONO…

① **Liceità, correttezza e trasparenza**
…trattati in modo lecito corretto e trasparente nei confronti dell'interessato

① **Limitazione della finalità:**
…raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità

② **Minimizzazione dei dati**
…adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati



ESATTEZZA

Art. 5.I dati personali oggetto di trattamento sono…

d) Esattezza e aggiornamento

…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

PRINCIPI GENERALI DEL TRATTAMENTO

Art. 5.I dati personali oggetto di trattamento sono:

e) **Limitazione della Conservazione**
…adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

f) **Integrità e riservatezza**
…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 accidentale.

I dati **devono essere conservati** in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per i quali sono trattati (salvo trattamenti archiviazione di pubblico interesse o per finalità di ricerca scientifica o per finalità statistiche)

Garantire adeguata sicurezza, protezione dei dati personali

PRINCIPI GENERALI DEL TRATTAMENTO

La violazione di cui agli artt: 5, 6, 7 e 9

- I diritti art. 12 a 22
- I trasferimenti di dati personali a un paese terzo da 44 a 49
- l'inosservanza ai sensi dell'art. 58 com. 2

È punita con sanzione amministrativa pecuniaria fino a **20.000.000** euro o fino al **4%** del fatturato mondiale annuo.

Comma 2

- Il Titolare del trattamento è **competente** per il rispetto del paragrafo 1 e in grado di **comprovarlo**

«Responsabilità»

*«devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti **rispetto alle finalità*** per le quali sono trattati»*

Metodologia di verifica e valutazione della qualità dei dati

Piano di campionamento per un'azienda che acquista data base. Ogni lotto è composto da 100 record.

-**Livello di ispezione generale**: Livello II
-**Lotto Campione:** 1 lotto = 100 record = 10.000 nominativi
-**Limite di qualità accettabile** : 1,0 (di norma definito da fornitore e cliente al momento della stipula del contratto)

Lotto campione	Livello ispezione generale		
	I	II	III
2 to 8	A	A	B
9 to 15	A	B	C
16 to 25	B	C	D
26 to 50	C	D	E
51 to 90	C	E	F
91 to 150	D	F	G
151 to 280	E	G	H
281 to 500	F	H	J
501 to 1.200	G	J	K
1.201 to 3.200	H	K	L
3.201 to 10.000	J	L	M
10.001 to 35.000	K	M	N
35.001 to 150.000	L	N	P
150.001 to 500.000	M	P	Q
500.001 over	N	Q	R

Lettera Codice	Numerosità campione	Limite di qualità accettabile (in %)					
		1,0	1,5	2,5	4,0	6,5	10,0
A	2	≤ 0	≤ 0	≤ 0	≤ 0	≤ 0	≤ 1
B	3	≤ 0	≤ 0	≤ 0	≤ 0	≤ 0	≤ 1
C	5	≤ 0	≤ 0	≤ 0	≤ 0	≤ 1	≤ 1
D	8	≤ 0	≤ 0	≤ 0	≤ 1	≤ 1	≤ 2
E	13	≤ 0	≤ 0	≤ 1	≤ 1	≤ 2	≤ 3
F	20	≤ 0	≤ 1	≤ 1	≤ 2	≤ 3	≤ 5
G	32	≤ 1	≤ 1	≤ 2	≤ 3	≤ 5	≤ 7
H	50	≤ 1	≤ 2	≤ 3	≤ 5	≤ 7	≤ 10
J	80	≤ 2	≤ 3	≤ 5	≤ 7	≤ 10	≤ 14
K	125	≤ 3	≤ 5	≤ 7	≤ 10	≤ 14	≤ 21
L	200	≤ 5	≤ 7	≤ 10	≤ 14	≤ 21	≤ 21
M	315	≤ 7	≤ 10	≤ 14	≤ 21	≤ 21	≤ 21
N	500	≤ 10	≤ 14	≤ 21	≤ 21	≤ 21	≤ 21
P	800	≤ 14	≤ 21	≤ 21	≤ 21	≤ 21	≤ 21
Q	1.250	≤ 21	≤ 21	≤ 21	≤ 21	≤ 21	≤ 21
R	2.000	≤ 21	≤ 21	≤ 21	≤ 21	≤ 21	≤ 21

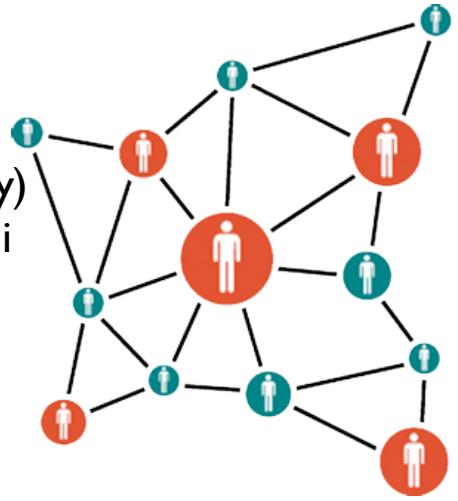
DATA MAPPING

- **REGISTRI DELLE ATTIVITA' DI TRATTAMENTO**

Il considerando 82 non ci chiarisce il punto

Il Regolamento nasce con la prospettiva di semplificare, responsabilizzando (Accountability) però il "Titolare" ma non ci fornisce indicazioni in merito

Si può presumere che rientri nei compiti del DPO?



E' quindi necessario prevedere **procedure** chiare ed **indicare nelle nomine/deleghe** chi provvederà alla stesura pratica del registro, chi lo aggiorna e come lo aggiorna.

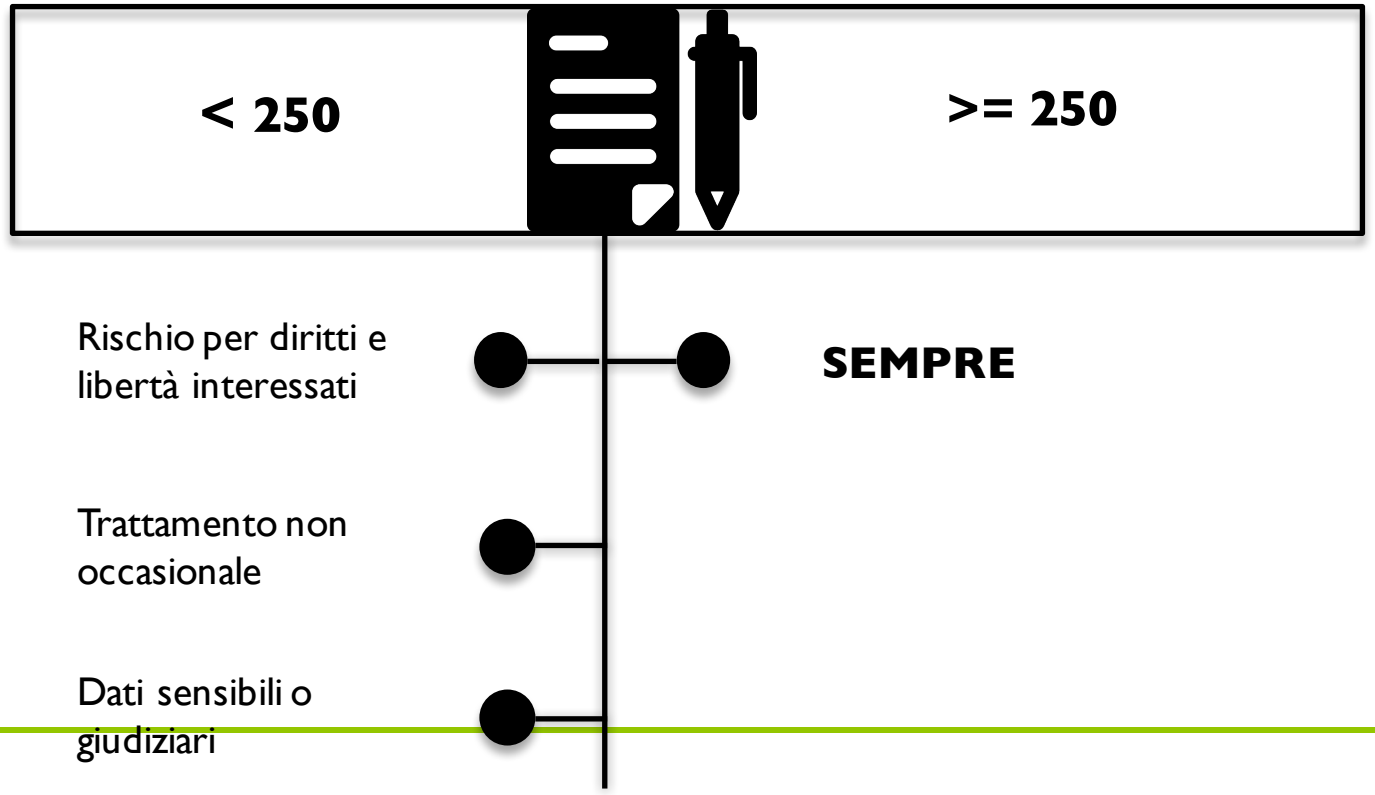
Inoltre è necessario pensare ad un meccanismo di verifica dell'accesso digitale controllato?

DATA MAPPING

- **REGISTRI DELLE ATTIVITA' DI TRATTAMENTO**

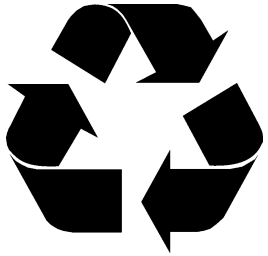
Obbligatorietà del registro dei trattamenti

Dipende dalla numerosità dei dipendenti dell'organizzazione:



VALUTAZIONE DEL RISCHIO

SICUREZZA DEI DATI PERSONALI



VALUTAZIONE DEI RISCHI

(art. 32 cons. 83)

VALUTAZIONE DEL RISCHIO

Art. 32 Comma 1

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

Il titolare e il **responsabile** del trattamento mettono in atto **misure tecniche** e **organizzative** **adeguate** per garantire un livello di sicurezza adeguato al rischio….

VALUTAZIONE DEL RISCHIO

Considerando 83)

Per mantenere la sicurezza e prevenire trattamenti in violazione del regolamento il **titolare** o il **responsabile** dovrebbero valutare i rischi inerenti al trattamento e attuare misure per limitare i rischi, *quali la cifratura*…

Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come:

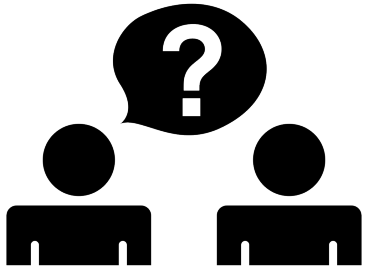
1. Distruzione accidentale (*significa per qualsiasi causa*)
2. Distruzione illegale
3. Perdita
4. Modifica
5. Rivelazione
6. Accesso non autorizzato a dati personali trasmessi, conservati o comunque elaborati

che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

IDENTIFICAZIONE, ANALISI, PONDERAZIONE, TRATTAMENTO

LE DOMANDE A CUI CERCA DI RISPONDERE

- **Che cosa può accadere ai dati personali e perché?**
- **Quali sono le conseguenze per i dati personali?**
- **Qual è la probabilità che l'evento si verifichi?**
- **Quali fattori possono mitigare le conseguenze del rischio sui dati Personali?**
- **Questi fattori possono ridurne la probabilità?**
- **Il livello di rischio sui dati personali è accettabile?**



il Fatto Quotidiano.it
Non riceve alcun finanziamento pubblico

Londra, clinica di Soho rivela per errore le identità di 780 sieropositivi

Mondo

A riportare la notizia è il Guardian. Ora l'autorità garante della privacy ora aprirà un'inchiesta sulla 56 Dean Street Clinic, che ha la sua sede nel cuore del quartiere gay della metropoli inglese

di Daniele Guido Gessa | 2 settembre 2015

Un miliardo di account Yahoo sono stati violati

L'attacco risale all'estate del 2013 e ha interessato anche migliaia di impiegati nelle più importanti agenzie governative statunitensi

Verizon, con un accordo da 4,8 miliardi di dollari, che dovrebbe essere concluso entro il primo trimestre del 2017.

…**Verizon aveva chiarito che ci sarebbero state conseguenze sull'accordo**, ventilando la possibilità di chiedere **uno sconto** o **di ritirarsi dall'affare**.

In seguito all'annuncio della nuova violazione su larga scala, Verizon ha diffuso un breve comunicato confermando la posizione di settembre: "Valuteremo la situazione man mano che Yahoo prosegue con le sue indagini. Prenderemo in considerazione le conseguenze di questi sviluppi prima di stringere un accordo definitivo".

MECCANISMI DI CERTIFICAZIONE & ODC

QUALI CAB RILASCIANO LA CERTIFICAZIONE?

CABs

REQUISITI:

- Possesso del livello adeguato di competenza riguardo alla protezione dei dati
- **EN-ISO/IEC 17065/2012**

RINNOVANO E RILASCIANO

DOPO AVER INFORMATO LE AUTORITA' DI CONTROLLO