Traning of Lawyers on the European Union's Data Protection Reform

TRADATA

Protezione dati, libera circolazione e altri diritti

Avv. Giuseppe Busia

Consiglio Nazionale Forense – 12 dicembre 2018

Il diritto alla protezione dei dati personali

- Dal diritto ad essere lasciati soli all'autodeterminazione informativa
- Un **diritto fondamentale**
  - Articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea
  - Articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE»)
- Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano
  - Indipendentemente da nazionalità o residenza
  - Un diritto «al servizio dell'uomo» (cons. 4)

Protezione dati e altri diritti

- Va contemperato con altri diritti fondamentali, in ossequio al principio di **proporzionalità**.
  - Non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale
- Libertà e i principi riconosciuti dalla Carta, sanciti dai Trattati, richiamati e oggetto di tutela
- In particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

Protezione dei dati e libera circolazione

- Il Regolamento generale «è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al **rafforzamento e alla convergenza delle economie** nel mercato interno e al benessere delle persone fisiche» (Considerando 2)

Mercato interno e flussi di dati

- L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole **aumento dei flussi transfrontalieri di dati personali** …tra attori pubblici e privati…(*Considerando 5*)
- Il **diritto dell'Unione impone** alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro.

Traning of Lawyers on the European Union's Data Protection Reform

TRADATA

Oggetto e Finalità del RGPD (Art. 1)

Avv. Giuseppe Busia

Consiglio Nazionale Forense – 12 dicembre 2018

Art. 1 (1-2)

- **1. Il regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati *(cfr. 3)***
- **2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.**

Art. 1 (3)

- 3. La libera circolazione dei dati personali nell'Unione
  - non può essere limitata
  - né vietata
- per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Traning of Lawyers on the European Union's Data Protection Reform

TRADATA

Dal Codice Privacy al Regolamento generale UE

Avv. Giuseppe Busia

Consiglio Nazionale Forense – 12 dicembre 2018

Una normativa in continua evoluzione

- Le leggi 31 dicembre 1996, nn. 675 e 676 e le successive deleghe
  - Dal diritto ad essere lasciati soli al controllo sui propri dati
- I decreti delegati fino al d.lgs. 467/2001
- Gli atti paranormativi e le pronunce del Garante
- **Il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196)**

Dalla Direttiva 95/46 al RGPD

- Sebbene i suoi obiettivi e principi rimangano **tuttora validi**, la **direttiva 95/46/CE non ha impedito la frammentazione** dell'applicazione della protezione dei dati … né ha eliminato la percezione.. che in particolare le operazioni online comportino rischi
- La compresenza di diversi livelli di protezione …negli Stati membri può ostacolare la libera circolazione dei dati personali... Tali differenze possono costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale **divario** ….**è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE** (Considerando 9)

Il Regolamento UE n. 679 del 2016

- **Il «pacchetto» con la direttiva ex Terzo pilastro**
  - Proposta della Commissione
  - L'iter di approvazione fra Parlamento e Consiglio
  - Il Gruppo ex art. 29 della Direttiva 95/46
  - La conclusione del Trilogo nel dicembre 2015
- **Una legge unica europea**
- **Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016**
  - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

Traning of Lawyers on the European Union's Data Protection Reform

TRADATA

Le principali novità del RGPD

Avv. Giuseppe Busia

Consiglio Nazionale Forense – 12 dicembre 2018

I pilastri della tutela nel vecchio Codice

- Informativa
- Consenso
  - Autorizzazione
    - Base normativa per soggetti pubblici (v. seguente)
- Diritti dell'interessato
- Misure di sicurezza
- Notificazione
  - Differenze col Regolamento Generale (rinvio)

Quadro generale del RGPD (1)

- **Responsabilizzazione del titolare**
  - Ciascuno si conosce meglio di quanto possa farlo l'Autorità
- **Valutazione di impatto sulla protezione dei dati**
  - Fin dalla progettazione del trattamento
    - Privacy by design
    - Privacy by default
- **Misure di sicurezza basate sul rischio**
  - Approccio basato sul rischio
  - Consultazione preventiva dell'Autorità

Quadro generale del RGPD (2)

- Codici di condotta (associativi)
- Responsabile della protezione dati (artt. 37 ss. - rinvio)
- Estensione obbligo di notifica all'Autorità delle violazioni dei dati personali (art. 33)
  - Senza ingiustificato ritardo e, ove possibile , entro 72 ore
  - Possibile comunicazione all'interessato

Quadro generale del RGPD (3)

- **Certificazione**
  - **La ripartizione dei ruoli ed i compiti dell'Autorità**
- **Sportello unico al quale rivolgersi**
  - **Possibili criticità per gli interessati**
  - **Individuazione dell'Autorità capofila in base allo stabilimento principale e altri criteri**
- **Sanzioni**
- **Diritti rafforzati**
  - **Portabilità, Oblio (rinvio)**

Traning of Lawyers on the European Union's Data Protection Reform

TRADATA

Ambito di applicazione

Avv. Giuseppe Busia

Consiglio Nazionale Forense – 12 dicembre 2018

Ambito di applicazione materiale

- Il RGPD si applica ai trattamenti:
  - interamente o parzialmente automatizzato di dati personali
  - non automatizzati di dati personali contenuti in un archivio o destinati a figurarvi
- Il regolamento (CE) n. 45/2001 disciplina i trattamenti svolti da istituzioni, organi, uffici e agenzie dell'Unione
  - Il processo di adeguamento (art. 98)
- Rinvio al Regolamento e-privacy

Quando il GDPR non si applica

Il GDPR non si applica ai trattamenti di dati personali:

- a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
- b) effettuati dagli Stati membri nell'ambito della politica estera e sicurezza comune (titolo V, capo 2, TUE);
- c) **effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale** o domestico; (C18)
- d) 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

Stabilimento principale (a)

- a) titolare con **stabilimenti in più di uno Stato membro**, il luogo della sua amministrazione centrale nell'Unione,
- **salvo che** le **decisioni sulle finalità e i mezzi** del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni
  - In quest'ultimo caso lo stabilimento che ha adottato tali decisioni è considerato stabilimento principale

Stabilimento principale (b)

- b) **responsabile** del trattamento con **stabilimenti in più di uno Stato membro**, il luogo in cui ha sede la sua amministrazione centrale nell'Unione
- **o,** se il responsabile non ha un'amministrazione centrale nell'Unione, lo stabilimento nell'Unione in cui sono condotte le **principali attività di trattamento** nel contesto delle attività di uno stabilimento del responsabile del trattamento
  - nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento

Ambito di applicazione territoriale (1)

- Trattamenti effettuati nell'ambito di uno stabilimento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione
  - Effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile
- Si applica anche al trattamento effettuato da un titolare che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico

Ambito di applicazione territoriale (2)

- Trattamenti riguardanti interessati che si trovano nell'Unione, effettuato da un **titolare o da un responsabile che non è stabilito nell'Unione**, quando le attività di trattamento riguardano:
- a) l'offerta di **beni o servizi a interessati nell'Unione**, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
- b) il **monitoraggio** del loro comportamento se tale comportamento ha luogo all'interno dell'Unione

Traning of Lawyers on the European Union's Data Protection Reform

TRADATA

Principi generali a confronto

Avv. Giuseppe Busia

Consiglio Nazionale Forense – 12 dicembre 2018

Alcuni principi generalissimi
(Art 11 Codice – Cfr Art. 5 RGPD)

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.

Principi applicabili ex Art. 5 (1)

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

- un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

(segue)

Principi applicabili ex Art. 5 (2)

d) 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) 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;

- i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)

(segue)

Principi applicabili ex Art. 5 (3)

f) 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»)

- **Il titolare del trattamento**
  - **È competente per il rispetto dei principi (paragrafo 1)**
  - **È in grado di comprovarlo**
    - **(«responsabilizzazione»).**

Traning of Lawyers on the European Union's Data Protection Reform

TRADATA

Le Regole Deontologiche

Avv. Giuseppe Busia

Consiglio Nazionale Forense – 12 dicembre 2018

I Codici di deontologia (1)

Differenze con i Codici di Condotta (art 40 RGPD – rinvio)

- Codici di deontologia e di buona condotta per determinati settori
- Il Garante promuove la sottoscrizione
  - Nell'ambito delle categorie interessate
  - Nell'osservanza del principio di rappresentatività
  - Tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa
- Verifica la conformità alle leggi ed ai regolamenti, anche attraverso l'esame di osservazioni di soggetti interessati

I Codici di deontologia (2)

- **Il rispetto di *tutti* è condizione essenziale per la liceità dei trattamenti**
  - **Anche il codice dei giornalisti**
- Pubblicati sulla Gazzetta Ufficiale
- Riportati in allegato al Codice privacy (allegato A)
  - Con decreto del Ministro della giustizia
- Il Garante contribuisce a garantirne la diffusione ed il rispetto

Le regole deontologiche (1)

Il Garante promuove, nell'osservanza del principio di rappresentatività e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni **di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al Capo IX del Regolamento** e ne verifica la conformità alle disposizioni vigenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

Le regole deontologiche (2)

- Lo schema di regole deontologiche è sottoposto a consultazione pubblica per almeno sessanta giorni.
- Le regole deontologiche sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente decreto.
- Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali.

Disposizione transitorie A5 A7

- Allegati A5 e A7 continuano a produrre effetti, sino alla definizione della procedura di cui alla lettera b), a condizione che si verifichino congiuntamente le seguenti condizioni:
- a) entro sei mesi le categorie interessate sottopongano all'approvazione del Garante, a norma dell'articolo 40 del Regolamento, i codici di condotta
- b) la procedura di cui alla lettera a) si concluda entro sei mesi dall'attivazione

Disposizione transitorie

- Allegati **A1, A2, A3, A4 e A6** sono **ridenominate regole deontologiche** e continuano a produrre effetti, in quanto compatibili con le disposizioni del Regolamento, e sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono successivamente riportate nell'allegato A) del presente decreto.
- Il Garante ne promuove la revisione sulla base delle disposizioni sulle regole di condotta

Disposizione transitorie A5 A7

- Allegati **A5 e A7** continuano a produrre effetti, sino alla definizione della procedura di cui alla lettera b), a condizione che si verifichino congiuntamente le seguenti condizioni:
- a) entro sei mesi le categorie interessate sottopongano all'approvazione del Garante, a norma dell'articolo 40 del Regolamento, i **codici di condotta**
- b) la procedura di cui alla lettera a) si concluda entro sei mesi dall'attivazione

Grazie dell’attenzione!

L'EFFETTO DELLA RIFORMA SULLA PROTEZIONE DEI DATI NEGLI STUDI LEGALI E IL RUOLO DEGLI ORDINI

The project is co-financed with the support of the European Union's Rights, Equality and Citizenship programme

Alcune figure…

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

OdV	RPCT	DPO	RSPP
D.Lgs. 231/2001	L. 190/2012	Reg. 2016/679	D.Lgs. 81/2008
MOG	PTPCT	GDPR + Registro dei trattamenti	DVR

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Risk Assessment

Risk Management

LA FORMULA DEL RISCHIO

Training of Lawyers on the European Data Protection Reform

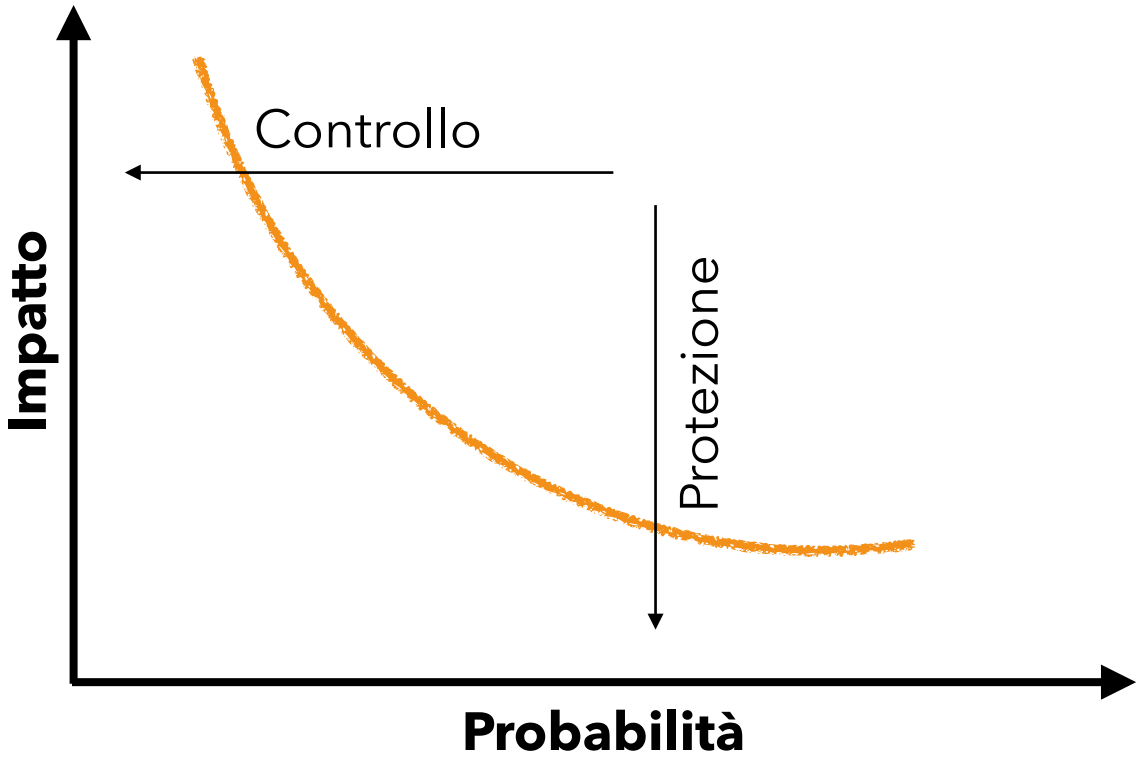
#TRADATA

Avv. Francesco Paolo Micozzi

R= P * Vu

Rischio = Probabilità * Impatto

Il rischio è l'effetto dell'incertezza sugli obiettivi



Training of Lawyers on the European Data Protection Reform

#TRADATA

GDPR
E OPPORTUNITÀ PER GLI AVVOCATI

Avv. Francesco Paolo Micozzi

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

GDPR
E OBBLIGHI PER GLI AVVOCATI

Avvocati verso il GDPR

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Consiglio Nazionale Forense
presso il Ministero della Giustizia

ACCEDI

CNF FONDAZIONI ORGANISMI AVVOCATI ARGOMENTI PUBBLICAZIONI CALENDARIO NEWS CONTATTI

Circolari e Comunicazioni

"Il GDPR e l'avvocato": linee guida per gli Avvocati in materia di Protezione dei Dati Personali

Il Regolamento UE 2016/679 relativo alla protezione dei dati personali sarà direttamente applicabile negli Stati membri a partire dal 25 maggio 2018.

Anche gli studi legali, indipendentemente dalla loro dimensione, dalla struttura e dall'area di attività dovranno adeguarsi

I dati ai quali l'avvocato nell'esercizio delle sue funzioni ha accesso sono, per loro natura, particolarmente sensibili: essi possono infatti riguardare la salute, l'orientamento religioso politico o sessuale, dati giudiziari, situazione familiare, dati di minori etc, ed il loro trattamento obbedisce ad una logica specifica, diversa da quella dell'impresa commerciale, essendo intimamente connessa al rapporto di fiducia che lega l'avvocato al suo cliente e al rispetto degli obblighi deontologici, primo fra tutti l'obbligo di garantire il segreto professionale.

La divulgazione, anche accidentale di tali dati potrebbe ledere i diritti e la libertà delle persone

http://www.consiglionazionaleforense.it/web/cnf/-/gdpr-avvocati-proget-1

Avvocati verso il GDPR

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Protezione dei Dati Personali
per gli Avvocati

Il GDPR e l'avvocato, Regolamento UE, modulistica

LEGGI TUTTO

Protezione dei Dati Personali
per gli Ordini

FAQ per gli Ordini, Regolamento UE, modulistica

LEGGI TUTTO

http://www.consiglionazionaleforense.it/web/cnf/-/gdpr-avvocati-proget-1

Avvocati verso il GDPR

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPEENS
AVOCATS EUROPEENS

Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10
Email : ccbe@ccbe.eu – www.ccbe.eu

CCBE Guidance on the main new compliance measures for lawyers regarding the General Data Protection Regulation (GDPR)

19/05/2017

With this paper the Council of Bars and Law Societies of Europe (CCBE)[1] wishes to provide an overview of the main new compliance measures that Bars and Law Societies may wish to recommend in order to ensure compliance with the requirements set out in the GDPR.

Avvocati e GDPR

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

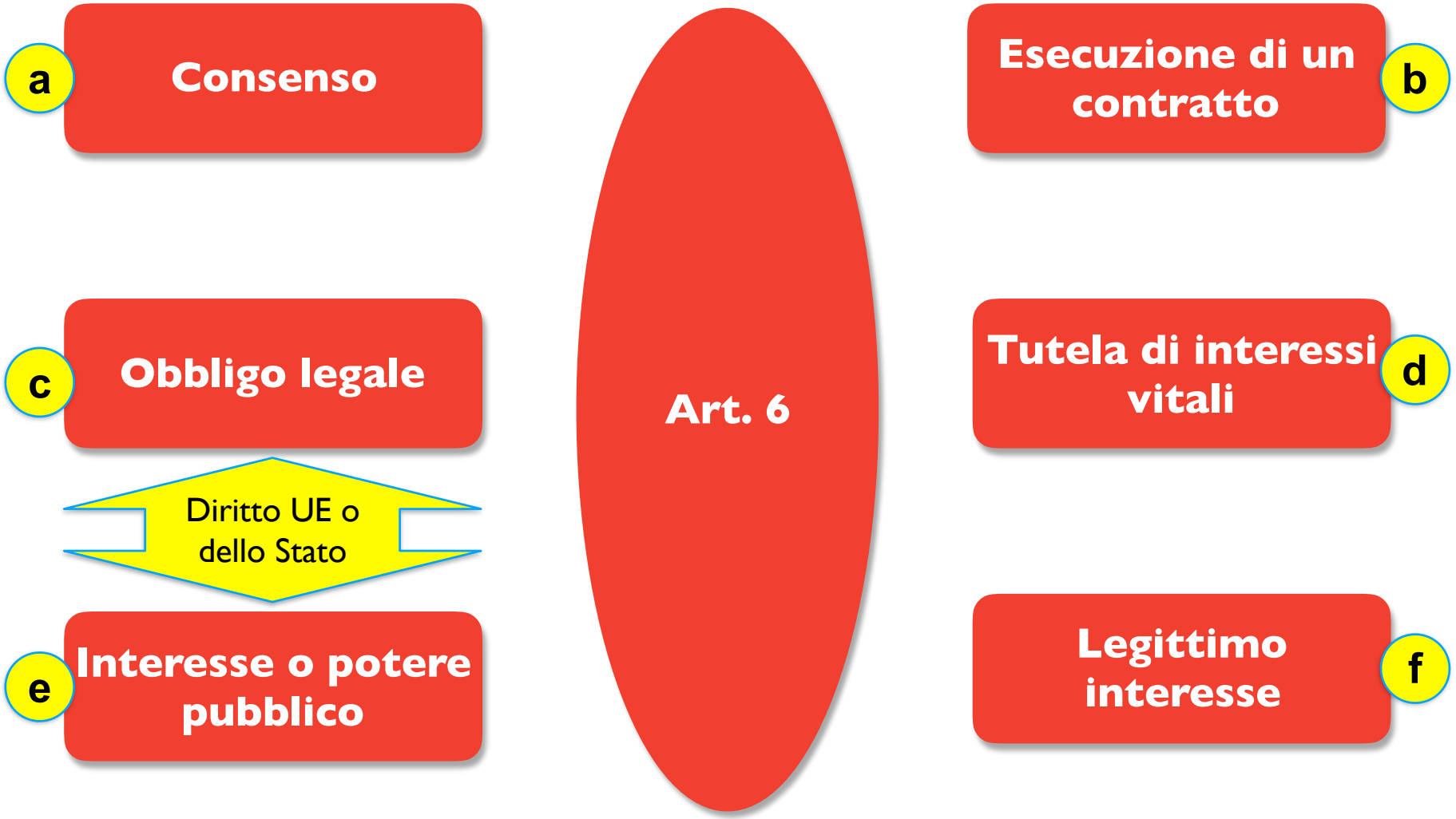
1. Analisi del flusso di trattamenti
2. "Organigramma" dello studio
3. **Informativa e altre policy**
4. **Creazione del Registro dei Trattamenti**
5. Verifica delle misure tecniche impiegate per ciascun trattamento
6. **Mettere in atto il sistema di segnalazione di data breach**
7. Eseguire la DPIA (ove richiesto)
7. **Prepararsi alla data portability**
9. Individuazione e nomina del DPO ?
10. **Verificare ipotesi di trattamenti transfrontalieri**
11. **Verifica contratti con responsabili del trattamento**

Le basi giuridiche sulle quali può legittimamente trattarsi il dato personale…

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi



soggetti

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

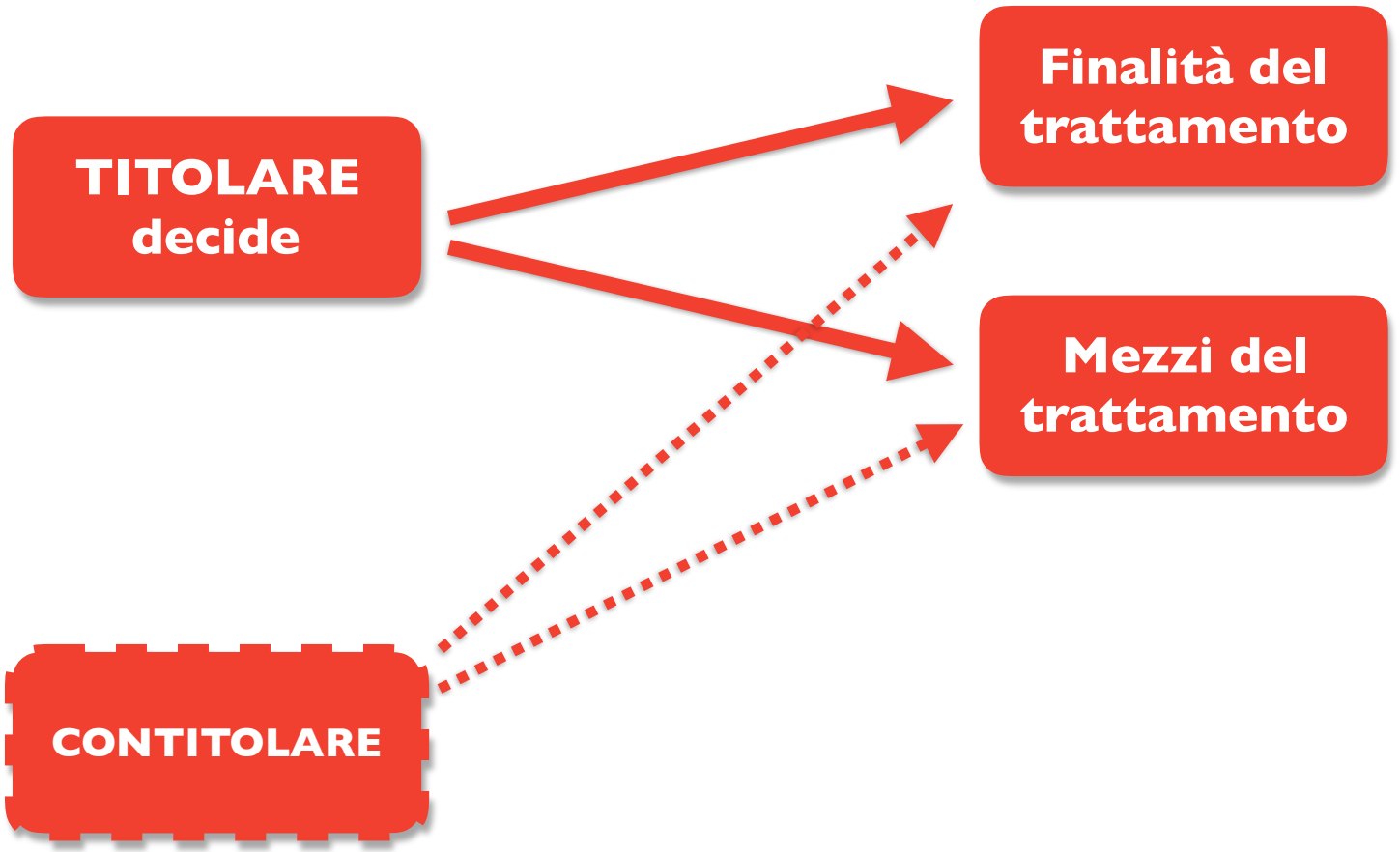
Italiano	Inglese	Francese
Titolare	Controller	Responsable du traitement
Responsabile del trattamento	Processor	Sous-traitant
Responsabile della protezione dei dati	Data Protection Officer	Délégué à la protection des données
Interessato	Data subject	Personne concernée
Autorità di controllo	Supervisory authority	Autorité de contrôle

Le figure soggettive - Titolare e contitolari

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi



Titolare, responsabile e sub-responsabile

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Art. 2-quaterdecies d.lgs. 196/03 (Attribuzione di funzioni e compiti a soggetti designati)

•1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che **specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità**.

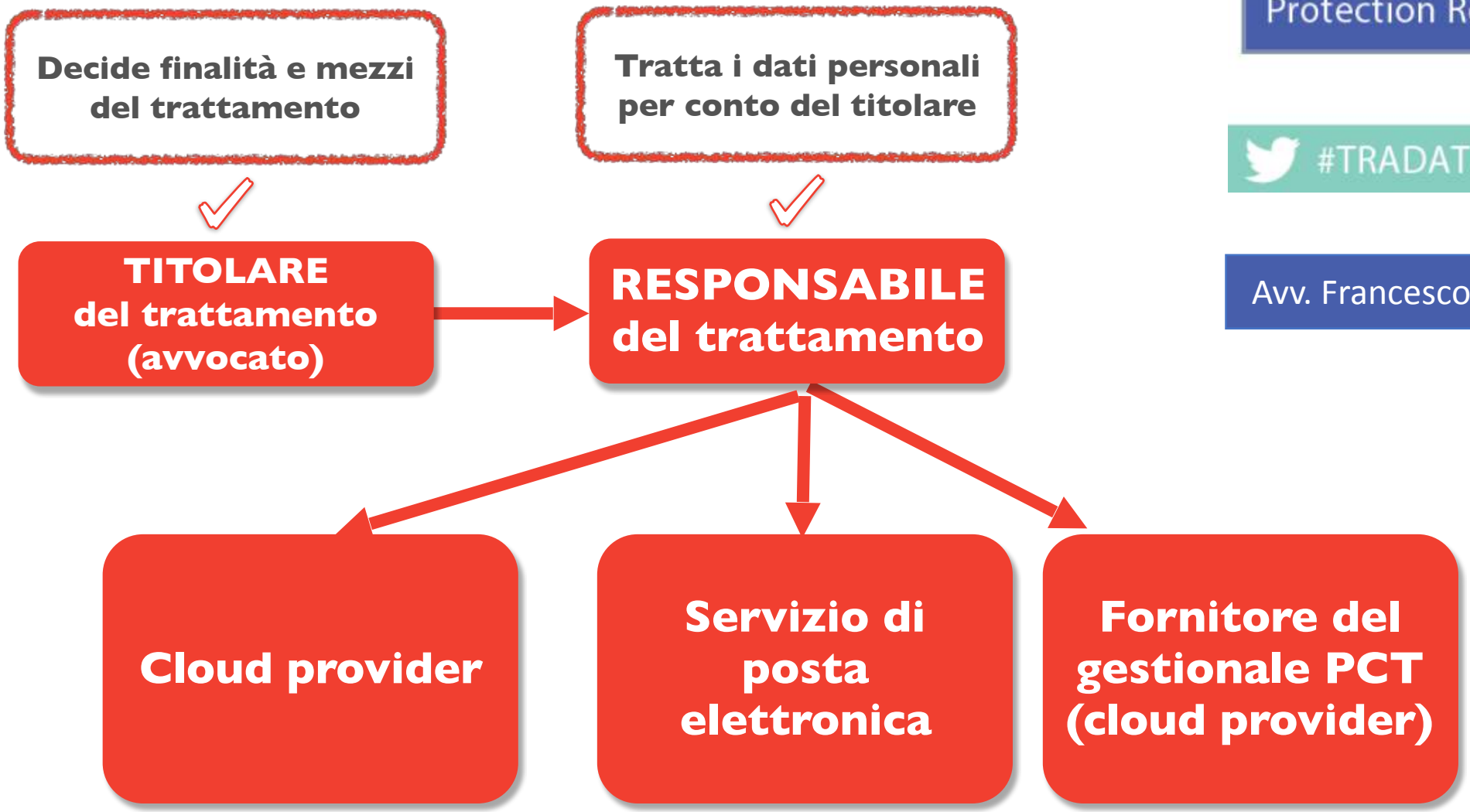
•2. Il titolare o il responsabile del trattamento individuano le modalità più opportune **per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta**.

Vediamo alcuni esempi

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi



Vediamo alcuni esempi

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

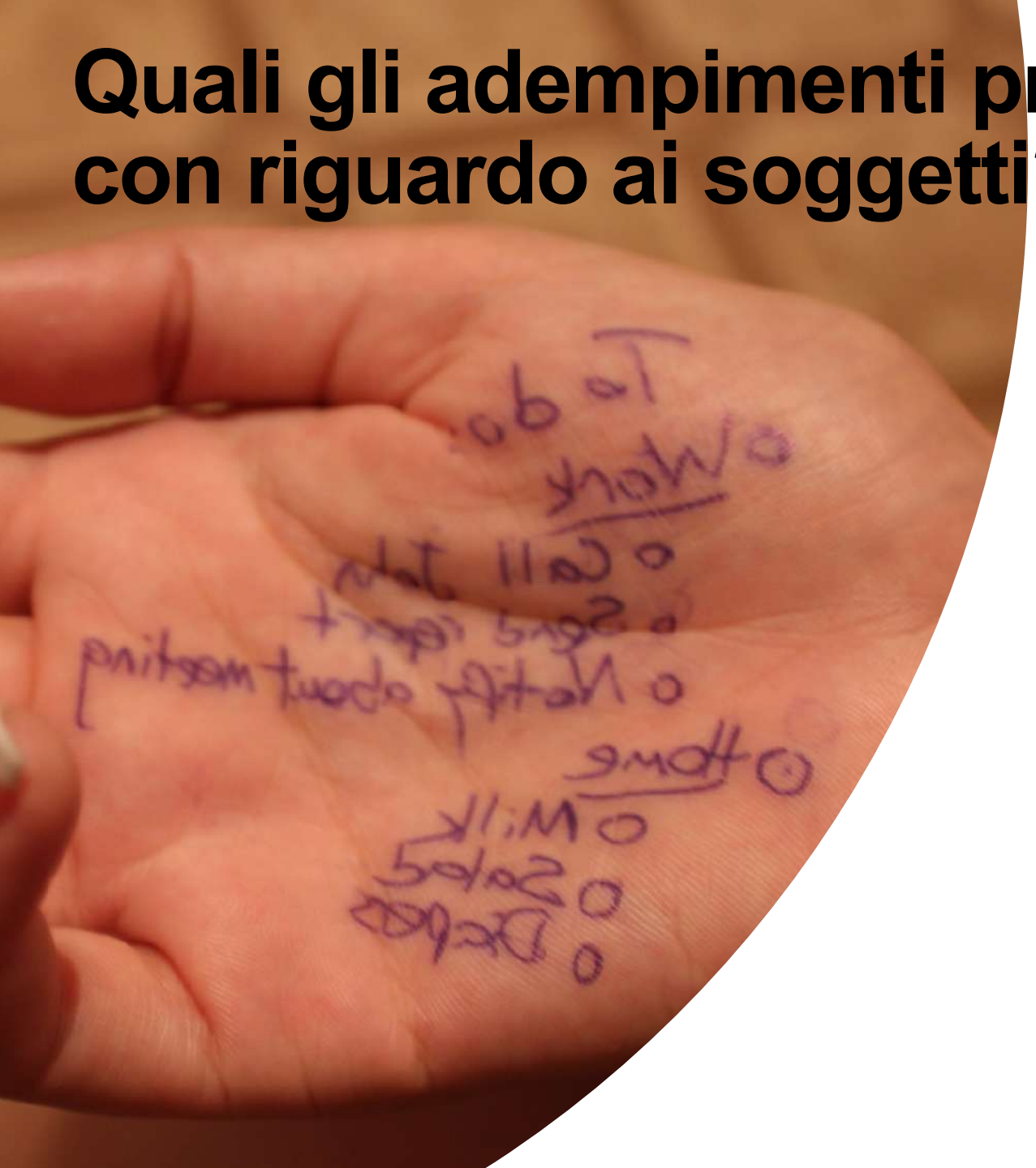
Gli autorizzati nello studio legale

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Quali gli adempimenti principali, con riguardo ai soggetti?



Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

- Accordi di contitolarità
- DPA con responsabili
- Delega compiti e funzioni
- Autorizzazioni e istruzioni
- Formazione
- Policy interne

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Informativa

In cosa resta uguale ad oggi?

- **l'informativa deve precedere il trattamento** (salvo i casi in cui i dati non siano raccolti presso l'interessato)

- **Il Titolare deve indicare:**
- **i propri dati e quelli dell'eventuale rappresentante nel territorio italiano**
- **le finalità del trattamento**
- **i diritti dell'interessato**
- **gli eventuali destinatari dei dati**

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Come cambia l'informativa nel GDPR?

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

- **Contenuti**
- **Dati di contatto del Data Protection Officer**
- **Base giuridica del trattamento**
- **Interesse legittimo al trattamento** (non applicabile alle PA)
- **Indicazione se sia previsto il trasferimento di dati in Paesi terzi**
  - **in caso affermativo: attraverso quali strumenti**
- **Periodo di conservazione dei dati**
  - **Nel caso non possa indicarsi il periodo preciso si dovrà, almeno, indicare i criteri stabiliti per stabilire la durata della conservazione**
- **Il diritto di presentare reclamo all'Autorità di controllo**
- **Si deve specificare se il trattamento comporta processi decisionali automatizzati e, nel caso, la logica dei processi decisionali e le possibili conseguenze per l'interessato**

Base giuridica del trattamento

- **Consenso al trattamento**
- **Il trattamento è necessario all'esecuzione di un contratto**
- **Il trattamento è necessario per adempiere un obbligo legale**
- **Il trattamento è necessario per la salvaguardia di interessi vitali**
- **Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri**
- **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 (non si applica alle PA)

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Consenso

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Diritti degli interessati

I diritti degli interessati

- **Trasparenza**
- **Informativa**
- **Diritto di accesso**
- **Diritto di rettifica**
- **Diritto alla cancellazione (oblio)**
- **Diritto di limitazione di trattamento**
- **Diritto alla portabilità dei dati** (consenso; contratto; mezzi automatizzati)
- **Diritto di opposizione**
- **Diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato**

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

I Registri delle attività di trattamento

Training of Lawyers on the European Data Protection Reform

#TRADATA

Data Protection By Default By Design

Avv. Francesco Paolo Micozzi

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Obblighi di sicurezza

Cosa è la sicurezza delle informazioni?

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

- **C - Confidenzialità**
- **I - Integrità**
- **A - Disponibilità**

Training of Lawyers on the European Data Protection Reform

#TRADATA

Avv. Francesco Paolo Micozzi

Data Breach

Training of Lawyers on the European Data Protection Reform

#TRADATA

Valutazione di impatto (DPIA)

Avv. Francesco Paolo Micozzi

GRAZIE PER L'ATTENZIONE!

The project is co-financed with the support of the European Union's Rights, Equality and Citizenship programme

Training of Lawyers on the EU Data Protection Reform (TRADATA)

The project is co-financed with the support of the European Union's Rights, Equality and Citizenship programme

Training of Lawyers on the European Data Protection Reform

#TRADATA

I diritti dell'interessato

Roma, 12 dicembre 2018

Avv. Nicola Fabiano
Componente Commissione Privacy CNF
Presidente UNIDPO

Training of Lawyers on the European Data Protection Reform

#TRADATA

Definizione e inquadramento di:

“Diritti dell’interessato”

Training of Lawyers on the European Data Protection Reform

#TRADATA

GDPR

Art. 1, par. 2:

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

Training of Lawyers on the European Data Protection Reform

#TRADATA

Considerando

(4) Il trattamento dei dati personali **dovrebbe essere al servizio dell'uomo**. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma **va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali**, in ossequio al principio di proporzionalità. Il presente regolamento **rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati**, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

Carta dei Diritti Fondamentali dell'Unione Europea

Training of Lawyers on the European Data Protection Reform

#TRADATA

Articolo 7
Rispetto della vita privata e della vita familiare

Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.

Articolo 8
Protezione dei dati di carattere personale

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Training of Lawyers on the European Data Protection Reform

#TRADATA

Breve ricostruzione storica della CDFUE

Si è detto che:

- ✓ *la riservatezza (art. 7 CDFUE)*
- ✓ *la protezione dei dati personali (art. 8 CDFUE)*

costituiscono diritti fondamentali nell'Unione europea

secondo la

(**Carta di Nizza** - **C**arta dei **D**iritti **F**ondamentali dell'**U**nione **E**uropea)

che è stata firmata appunto a Nizza il 7 dicembre 2000 e poi adattata il 12 dicembre 2007 a Strasburgo.

La Carta si compone di complessivi 54 articoli ed è strutturata come segue:

Titolo I - Dignità (artt. 1-5)
Titolo II - Libertà (artt. 6-19)
Titolo III - Uguaglianza (artt. 20-26)
Titolo IV - Solidarietà (artt. 27-38)
Titolo V - Cittadinanza (artt. 39-46)
Titolo VI - Giustizia (artt. 47-50)
Titolo VII - Disposizioni generali … (artt. 51-54)

I diritti in questione sono previsti nel Titolo II - ***Libertà***.

Prima della Carta di Nizza (CDFUE) qual era il riconoscimento dei diritti fondamentali ?

Sostanzialmente la giurisprudenza della Corte di Giustizia dell'Unione Europea (CGUE), poiché il Trattato di Roma nulla diceva sui diritti fondamentali e successivamente quello di Maastricht formulava unicamente una enunciazione.

Cosa accadde dopo la Carta di Nizza ?

Il 13 dicembre 2007 veniva firmato il trattato di Lisbona - TUE (entrato in vigore il dì 1 dicembre 2009) che all'articolo 6, paragrafo 1, stabilisce:

"*L'Unione riconosce i diritti, le libertà e i principi sanciti nella* ***Carta dei diritti fondamentali dell'Unione europea*** *del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati*".

Quindi

la **CDFUE** ha valore di trattato, fonte primaria del diritto dell'Unione e giuridicamente vincolate per ogni Stato membro

- ✓ ***Corte di giustizia - CGUE*** *(ha sede a Lussemburgo e competenza sul rispetto dei trattati) e*

- ✓ ***Corte EDU - CEDU*** *(istituita dall'art. 19 della Convenzione europea dei diritti dell'uomo ha sede a Strasburgo)*

Training of Lawyers on the European Data Protection Reform

#TRADATA

Ubi societas, ibi ius

La questione della prevalenza

dello Stato sull'individuo

Training of Lawyers on the European Data Protection Reform

#TRADATA

Breve introduzione sui diritti della personalità

Cosa intendiamo per “diritti della personalità” ?

Si tratta di situazioni giuridiche soggettive, tutelate dall’ordinamento e relative agli attributi essenziali della personalità di un soggetto giuridico (*P. Stanzione*). In particolare, la personalità costituisce un bene giuridicamente rilevante e meritevole di tutela secondo l’ordinamento giuridico che afferisce direttamente alla persona umana (dinamico e non statico).

La matrice può considerarsi antica.

Tuttavia, nell'ordinamento giuridico recente emergono i seguenti principali riferimenti:

Costituzione

Art. 2 - "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale"

Art. 13 - "La liberta`personale è inviolabile".

Art. 14 - "Il domicilio è inviolabile"

Art. 15 - "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili"

…

Art. 24, c. 2, - "La difesa è diritto inviolabile in ogni stato e grado del procedimento"

Codice Civile

Art. 5 c.c. - Atti di disposizione del proprio corpo
Art. 7 c.c. - Tutela del nome
Art. 9 c.c. - Tutela dello pseudonimo
Art. 10 c.c. Tutela dell'immagine

Training of Lawyers on the European Data Protection Reform

#TRADATA

Che qualificazione si può attribuire ai diritti fondamentali e a quelli della personalità ?

❊ ❊ ❊ ❊ ❊

La sovranità dell'individuo rispetto allo Stato ?

Training of Lawyers on the European Data Protection Reform

#TRADATA

«L'uomo è nato libero e ovunque si trova in catene»

(Contratto Sociale, 1762, Libro I, cap.1)

Jean-Jacques Rousseau

Qualificazione

Training of Lawyers on the European Data Protection Reform

#TRADATA

Identità personale = coscienza di sé

PIENA CONSAPEVOLEZZA

del valore del dato personale

* * * * *

Mercificazione dei dati personali

Training of Lawyers on the European Data Protection Reform

#TRADATA

Diritti dell'interessato

CAPO III - Diritti dell'interessato (Artt. 12-22)

Training of Lawyers on the European Data Protection Reform

#TRADATA

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 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

Altri diritti nel GDPR

Training of Lawyers on the European Data Protection Reform

#TRADATA

Articolo 23 - *Limitazioni*

2. h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

Articolo 34 - *Comunicazione di una violazione dei dati personali all'interessato*

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*

1. L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, …

Articolo 82 - *Diritto al risarcimento e responsabilità*

Training of Lawyers on the European Data Protection Reform

#TRADATA

Regole procedurali (art. 12)

Training of Lawyers on the European Data Protection Reform

#TRADATA

Soggetto tenuto: il titolare
Specifiche azioni: adotta misure appropriate
Obblighi del titolare:

- ✓ agevola l'esercizio dei diritti dell'interessato
- ✓ fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 (sono escluse altre richieste);
- ✓ nei casi di cui all'art. 11, par. 2, il titolare non può rifiutare la richiesta dell'interessato

Termine: senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (consentita proroga di 2 mesi ma il titolare deve informare l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta);

Se non ottempera: il titolare informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale;

Diritto di accesso (art. 15)

Training of Lawyers on the European Data Protection Reform

#TRADATA

Collocazione sistematica subito successiva agli articoli sulle informazioni (13-14)

A chi va rivolta la richiesta: al titolare del trattamento

Oggetto della richiesta: la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano (è esclusa la "modalità" del trattamento);

Forma della richiesta: analogica / digitale - forma libera;

Informazioni oggetto della richiesta: lettere dalla a) alla h) del par. 1 dell'art. 15;

Ipotesi di trasferimento di dati a un paese terzo: esistenza di garanzie adeguate;

Modalità di evasione della richiesta:

- ✓ il titolare fornisce per iscritto o con altri mezzi, anche con mezzi elettronici copia dei dati personali oggetto di trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12);
- ✓ Il responsabile collabora con il titolare (ex art. 28, par. 3, lett. e)

Termine di evasione: senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (v. art. 12).

Diritto di rettifica (art. 16)

Training of Lawyers on the European Data Protection Reform

#TRADATA

Soggetto richiedente: interessato;

A chi va rivolta la richiesta: al titolare del trattamento;

Oggetto della richiesta: la rettifica dei dati personali che riguardano l'interessato (può fornire dichiarazione integrativa);

Forma della richiesta: analogica / digitale - forma libera;

Modalità di evasione:

- ✓ il titolare fornisce la risposta in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12);
- ✓ il responsabile collabora con il titolare (ex art. 28, par. 3, lett. e)

Termine di evasione: senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (v. art. 12).

Diritto alla cancellazione (art. 17)

Training of Lawyers on the European Data Protection Reform

#TRADATA

Soggetto richiedente: interessato

A chi va rivolta la richiesta: al titolare del trattamento

Oggetto della richiesta: la cancellazione dei dati personali che riguardano l'interessato;

Forma della richiesta: analogica / digitale - forma libera;

Motivi (art. 17, par. 2) lettere dalla a) alla f):

Condizioni:

✓ se ha reso pubblici dati personali (art. 17, par. 2);

Modalità di evasione:

✓ il titolare fornisce la risposta in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12);

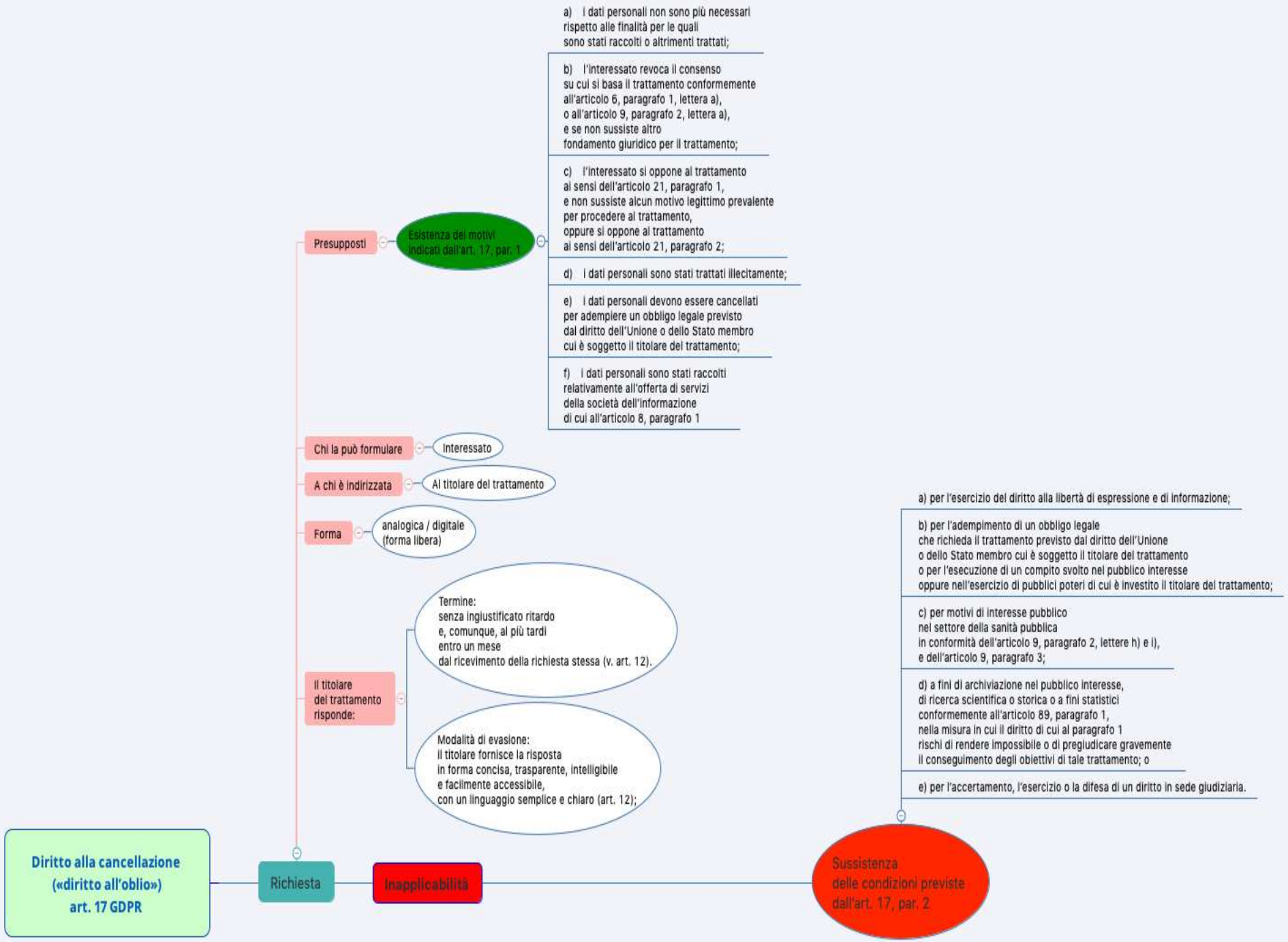
✓ Il responsabile collabora con il titolare (ex art. 28, par. 3, lett. e)

Termine di evasione: senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (v. art. 12).

Inapplicabilità: se il trattamento sia necessario secondo l'art. 17, par. 3;

Training of Lawyers on the European Data Protection Reform

#TRADATA



Diritto di limitazione di trattamento (art. 18)

Training of Lawyers on the European Data Protection Reform

#TRADATA

Soggetto richiedente: interessato
A chi va rivolta la richiesta: al titolare del trattamento
Oggetto della richiesta: la limitazione del trattamento
Forma della richiesta: analogica / digitale - forma libera;
Condizioni (art. 18, par. 1, lettere dalla a alla d) :
Modalità di evasione:

- ✓il titolare informa l'interessato, fornendo la risposta in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12);
- ✓Il responsabile collabora con il titolare (ex art. 28, par. 3, lett. e)

Termine di evasione: senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (v. art. 12).

Conseguenze:

- ✓i dati non si possono conservare
- ✓il trattamento è consentito solo:
  - ➢per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure
  - ➢per tutelare i diritti di un'altra persona fisica o giuridica o
  - ➢per motivi di interesse pubblico rilevante

Diritto alla portabilità (art. 20)

Training of Lawyers on the European Data Protection Reform

#TRADATA

WP 242 rev.01
Guidelines on the right to data portability

Soggetto richiedente: interessato
A chi va rivolta la richiesta: al titolare del trattamento
Oggetto della richiesta: ricevere i propri dati personali in formato strutturato
Forma della richiesta: analogica / digitale - forma libera;
Diritto di trasmettere i dati ad altro titolare (art. 20, par. 1) qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'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.

Modalità di evasione:

- ✓ il titolare informa l'interessato, fornendo la risposta in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12);
- ✓ Il responsabile collabora con il titolare (ex art. 28, par. 3, lett. e)
- ✓ il titolare trasmette, se tecnicamente fattibile, i dati personali ad altro titolare

Termine di evasione: senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (v. art. 12).
Diritto alla cancellazione: sempre consentito
Inapplicabilità:

- ✓ Il diritto alla portabilità non si applica al trattamento 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.

Diritto di opposizione (art. 21)

Training of Lawyers on the European Data Protection Reform

#TRADATA

Soggetto richiedente: interessato
A chi va rivolta la richiesta: al titolare del trattamento
Oggetto della richiesta: opposizione al trattamento dei dati personali
Forma della richiesta: analogica / digitale - forma libera;
Motivi: connessi alla sua situazione particolare ai sensi dell'art. 6, par. 1, lett. e) e f)
Modalità di evasione:

- ✓ il titolare informa l'interessato, fornendo la risposta in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12);
- ✓ Il responsabile collabora con il titolare (ex art. 28, par. 3, lett. e)
- ✓ il titolare si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

Termine di evasione: senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (v. art. 12).
Se per finalità di marketing: diritto ad opporsi in qualsiasi momento
Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89: sussiste il diritto di opporsi salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico

Diritto di non essere sottoposto (art. 22)

Training of Lawyers on the European Data Protection Reform

#TRADATA

Soggetto richiedente: interessato
A chi va rivolta la richiesta: al titolare del trattamento
Oggetto della richiesta: non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona.
Forma della richiesta: analogica / digitale - forma libera;
Eccezioni: art. 21, par. 1, non si applica se la decisione rientra nella previsione dell'art. 21, par. 1, lett. a), b) e c)
Modalità di evasione:

- ✓ il titolare informa l'interessato, fornendo la risposta in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12);
- ✓ Il responsabile collabora con il titolare (ex art. 28, par. 3, lett. e)
- ✓ il titolare provvede

Termine di evasione: senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (v. art. 12).
Se la decisione è necessaria per l'esecuzione di un contratto o è basata sul consenso: il titolare attua misure appropriate, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione
Esclusione delle categorie particolari di dati (art. 21, par. 4)

WP 251 rev.01
Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679

Training of Lawyers on the European Data Protection Reform

#TRADATA

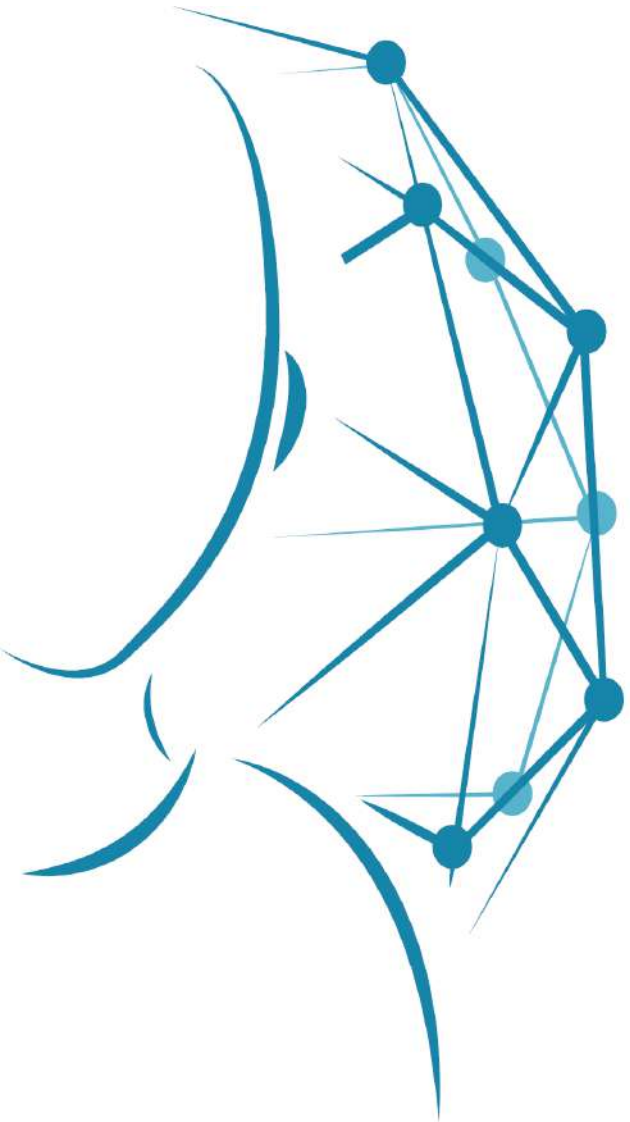
Etica

Cosa si intende per “etica” ?

Genericamente, la contrapposizione tra bene e male, giusto e sbagliato

Training of Lawyers on the European Data Protection Reform

#TRADATA



DEBATING ETHICS:

DIGNITY AND RESPECT IN DATA DRIVEN LIFE

40th International Conference

of Data Protection and Privacy Commissioners

Training of Lawyers on the European Data Protection Reform

#TRADATA

Training of Lawyers on the European Data Protection Reform

#TRADATA

ICDPPC

International Conference of Data Protection & Privacy Commissioners

DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE

40th International Conference of Data Protection and Privacy Commissioners

Tuesday 23rd October 2018, Brussels

The 40th International Conference of Data Protection and Privacy Commissioners **considers that** any creation, development and use of artificial intelligence systems **shall fully respect human rights, particularly the rights to the protection of personal data and to privacy, as well as human dignity, non-discrimination and fundamental values,** and shall provide solutions to allow individuals to maintain control and understanding of artificial intelligence systems.

Giovanni Buttarelli (EDPS)
Speech 24/10/2018

Training of Lawyers on the European Data Protection Reform

#TRADATA

Privacy is a universal value.

…

What do I mean by ethics?

Ethics is the sense we all have, often subconscious, of right and wrong in different circumstances.

Philosophers on this stage will shortly explain how ethical consensuses have emerged in the past.

In today's digital sphere, however, there is no such ethical consensus.

We do not have a consensus in Europe, and we certainly do not have one at a global level.

But we urgently need one.

…

What then is the relationship of ethics and the law?

It is fair to say that the early reactions to this idea of a global debate on ethics were mixed.

From my perspective, ethics come before, during and after the law.

It informs how laws are drafted, interpreted and revised. It fills the gaps where the law appears to be silent.

Ethics is the basis for challenging laws.

Remember that slavery was legal.

Child labour and censorship are still legal in many jurisdictions.

We tackle these injustices on the basis of ethics.

Tim Cook (CEO di Apple)
Speech 24/10/2018

Training of Lawyers on the European Data Protection Reform

#TRADATA

In ogni fase del processo creativo, allora e ora, **ci impegniamo in un dibattito etico aperto, onesto e solido sui prodotti che realizziamo e sull'impatto che avranno**. Questa è solo una parte della nostra cultura. Non lo facciamo perché dobbiamo farlo, lo facciamo perché dovremmo. […] Comprendiamo che i pericoli sono reali, dai cyber-criminali agli stati nazione canaglia. […]
Quei valori ... quell'impegno nel dibattito ponderato e nella trasparenza ... diventeranno sempre più importanti. Man mano che i progressi accelerano, queste cose dovrebbero continuare a radicarci e connetterci, prima di tutto, alle persone che serviamo. […]
[…]
Tuttavia, far progredire l'intelligenza artificiale raccogliendo enormi profili personali è pigrizia, non efficienza. **Perché l'Intelligenza Artificiale sia veramente intelligente, deve rispettare i valori umani, compresa la privacy.** Se ci sbagliamo, i pericoli sono profondi. Siamo in grado di ottenere sia grande Intelligenza Artificiale che ottimi standard di privacy. **Non è solo una possibilità, è una responsabilità. Nel perseguimento dell'intelligenza artificiale, non dovremmo sacrificare l'umanità, la creatività e l'ingegno che definiscono la nostra intelligenza umana.**

Isabelle Falque-Pierrotin (ICDPPC Chair) Speech 25/10/2018

Training of Lawyers on the European Data Protection Reform

#TRADATA

Questa crisi immediata è quella di una **sensazione di perdita di controllo sui dati personali** […]. Questa "crisi dei dati" non è solo una crisi di fiducia nell'uso dei dati personali. **È la sensazione che sia stata costruita un'intera società digitale senza di noi**: che questa società digitale stia facendo delle scelte sulle libertà, sulle organizzazioni, sulla visione politica e che non siamo più padroni di queste scelte.
In questo contesto, l'interrogatorio etico è legittimo, e non è limitato alla nostra assemblea da solo, dobbiamo essere consapevoli.
L'interrogativo etico è il significato che vogliamo dare al nostro mondo. Si occupa anche del metodo per costruire questo significato.
Se non rispondiamo a queste due domande, se non agiamo attraverso decisioni concrete ed efficaci, non possiamo tenere collettivamente le mani sul nostro futuro. E c'è urgenza e una forte aspettativa dei nostri concittadini sull'argomento. **Ma non chiuderci in un concetto di etica troppo teorica che alla fine diventerebbe il rivestimento della nostra inazione o impotenza. Agire ora!**
Perché l'etica non può essere un principio guida, né uno standard comune, purché non sia un riflesso di un contratto collettivo - non solo tra noi, regolatori, ma tra i diversi stakeholder che compongono la nostra società. L'etica sta costruendo uno spazio comune di dialogo e prendendo decisioni basate su questa comune riflessione….

Training of Lawyers on the European Data Protection Reform

#TRADATA

E’ possibile una “lettura” etica del GDPR ?

I Principi nel GDPR

Training of Lawyers on the European Data Protection Reform

#TRADATA

- «liceità, correttezza e trasparenza» (art. 5.1a);
- «limitazione della finalità» (art. 5.1b);
- «minimizzazione dei dati» (art. 5.1c);
- «esattezza» (art. 5.1d);
- «limitazione della conservazione» (art. 5.1e);
- «integrità e riservatezza» (art. 5.1f);
- «resposabilizzazione (accountability)» (art. 5.2);

WP260 rev.01
Linee guida sulla trasparenza ai sensi del regolamento 2016/679

Training of Lawyers on the European Data Protection Reform

#TRADATA

Grazie per l'attenzione

Avv. Nicola Fabiano

info@fabiano.law

www.fabiano.law

@nicfab

/nicfab

/nicfab

TRADATA

Training of Lawyers on the European Union's Data Protection Reform

12 dicembre 2018

Consiglio Nazionale Forense, Via del Governo Vecchio, 3, Roma

Primo evento formativo in Italia di un ciclo di seminari internazionali sulla riforma della protezione dei dati dell'UE il seminario si incardina nell'ambito delle iniziative dedicate alla cultura e sensibilizzazione in materia di protezione dei dati personali del Consiglio Nazionale Forense, come il Corso di alta formazione "corsodpo.it". Progetto europeo coordinato dalla European Lawyers Foundation (ELF) del CCBE, con partner i Consigli nazionali e le Law society di Belgio, Francia, Germania, Irlanda, Irlanda del Nord, Inghilterra e Galles, e Spagna, che prevede la formazione di almeno 650 avvocati di 8 giurisdizioni.

11:30 – 12:30 **Accountability, sicurezza e data breach**

Avv. Giovanni Battista Gallus - *Componente Commissione privacy CNF*

Training of Lawyers on the European Data Protection Reform

#TRADATA

Responsabilizzazione (accountability)

Misure adeguate e efficaci per garantire i principi e gli obblighi

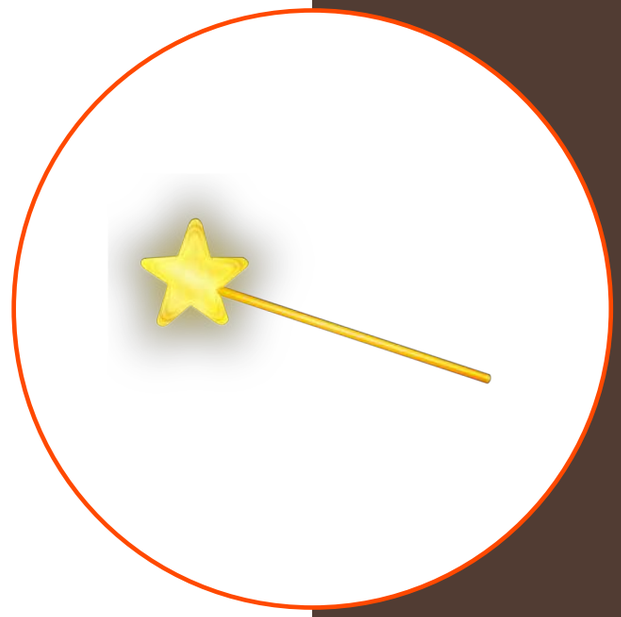
Accountability

Adattabilità

Dimostrazione dell'osservanza degli obblighi

One size fits all?

- *"**Non esistono alternative valide alle soluzioni "su misura"**. Infatti, le misure specifiche da applicare devono essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare attenzione al rischio inerente al trattamento e al tipo di dati. **Un approccio uguale per tutti** avrebbe il solo effetto di costringere i responsabili del trattamento all'interno di strutture inadatte e **si rivelerebbe** quindi **fallimentare**"*



- Art. 29WP, Parere 3/2010 - WP 173

Training of Lawyers on the European Data Protection Reform

#TRADATA

Gli strumenti dell'accountability

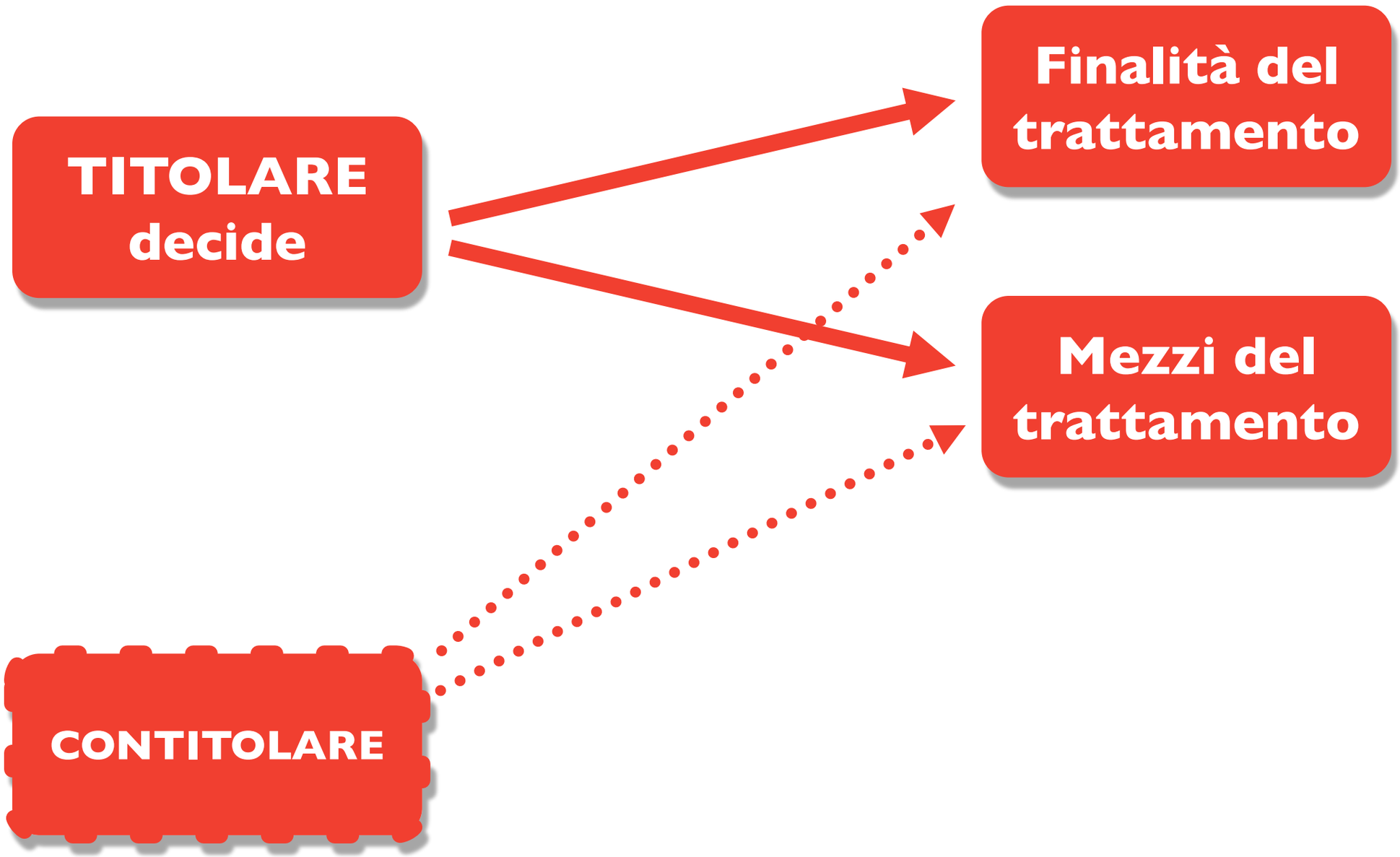
- Organigramma coerente
- Misure organizzative
- Registro dei trattamenti
- Valutazione di impatto privacy
- Privacy by design/by default
- Misure di sicurezza
- Regolamentazione dei data breach
- Designazione di un RPD/DPO
- Codici di condotta/certificazione trattamenti??

Training of Lawyers on the European Data Protection Reform

#TRADATA

i soggetti

Le figure soggettive - Titolare e contitolari



Le figure soggettive - Titolare e contitolari

• Art. 4, n. 7 - **«titolare del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

• Art. 26 - **Contitolari**: due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento

Titolare, responsabile e sub-responsabile

Decide finalità e mezzi del trattamento

TITOLARE del trattamento

“AUTORIZZATI” al trattamento

Gli “autorizzati” possono essere organizzati con diversi livelli di delega (designati/autorizzati)

Tratta i dati personali per conto del titolare

RESPONSABILE del trattamento

“AUTORIZZATI” al trattamento

Gli “autorizzati” possono essere organizzati con diversi livelli di delega (designati/autorizzati)

Tratta i dati personali su incarico del responsabile e per conto del titolare

SUBRESPONSABILE del trattamento

“AUTORIZZATI” al trattamento

Gli “autorizzati” possono essere organizzati con diversi livelli di delega (designati/autorizzati)

Art. 2-quaterdecies d.lgs. 196/03 (Attribuzione di funzioni e compiti a soggetti designati)

• 1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che **specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità**.

• 2. Il titolare o il responsabile del trattamento individuano le modalità più opportune **per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta**.

Vediamo alcuni esempi

Decide finalità e mezzi del trattamento

✓

TITOLARE del trattamento (avvocato)

Tratta i dati personali per conto del titolare

✓

RESPONSABILE del trattamento

Cloud provider

Servizio di posta elettronica

Fornitore del gestionale PCT (cloud provider)

Vediamo alcuni esempi

Decide finalità e mezzi del trattamento

✓

TITOLARE del trattamento (avvocato)

Tratta i dati personali per conto del titolare

✓

RESPONSABILE del trattamento (commercialista/Consulente del lavoro)?

Titolari autonomi, contitolari o responsabili?

Gli autorizzati nello studio legale

Decide finalità e mezzi del trattamento

TITOLARE del trattamento

Designati (delega compiti e funzioni)

Praticanti

“AUTORIZZATI” al trattamento

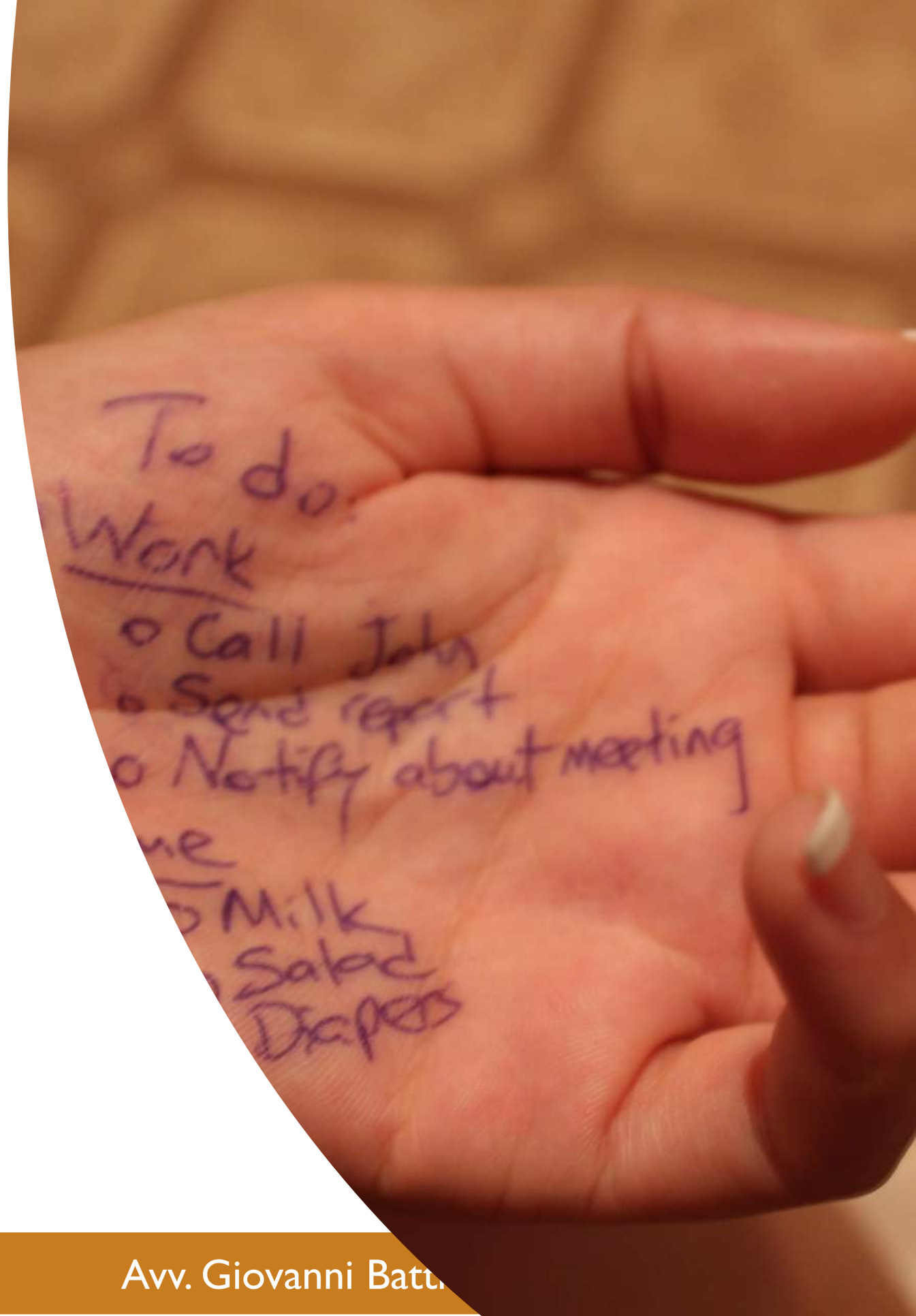
Addetti alla segreteria

Stagisti/Collaboratori

Gli “autorizzati” possono essere organizzati con diversi livelli di delega (designati/autorizzati)

Quali gli adempimenti principali, con riguardo ai soggetti?

- Accordi di contitolarità
- DPA con responsabili
- Delega compiti e funzioni
- Autorizzazioni e istruzioni
- Formazione
- Policy interne



Training of Lawyers on the European Data Protection Reform

#TRADATA

La nascita di una nuova figura: il DPO

Art. 37, comma 5 - Requisiti del DPO

Conoscenza specialistica di norme su privacy e data protection

Capacità di assolvere ai compiti previsti dall'art. 39

Training of Lawyers on the European Data Protection Reform

#TRADATA

Compiti del DPO

Compiti del DPO

offre consulenza a titolare, responsabile e dipendenti

fornisce il parere (se richiesto) sul DPIA

sorveglia sul rispetto della disciplina sulla protezione dati

coopera con l'Autorità di controllo

funge da punto di contatto per l'autorità di controllo

valuta i rischi che incombono sui dati personali trattati

Rapporti tra DPO e interessati

Art. 38 - Posizione del responsabile della protezione dei dati

*4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le **questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti** derivanti dal presente regolamento.*

DPO come opportunità - I dati del Garante

Comunicazioni dei dati di contatto degli RPD **40.738**

Reclami e segnalazioni **2.547**

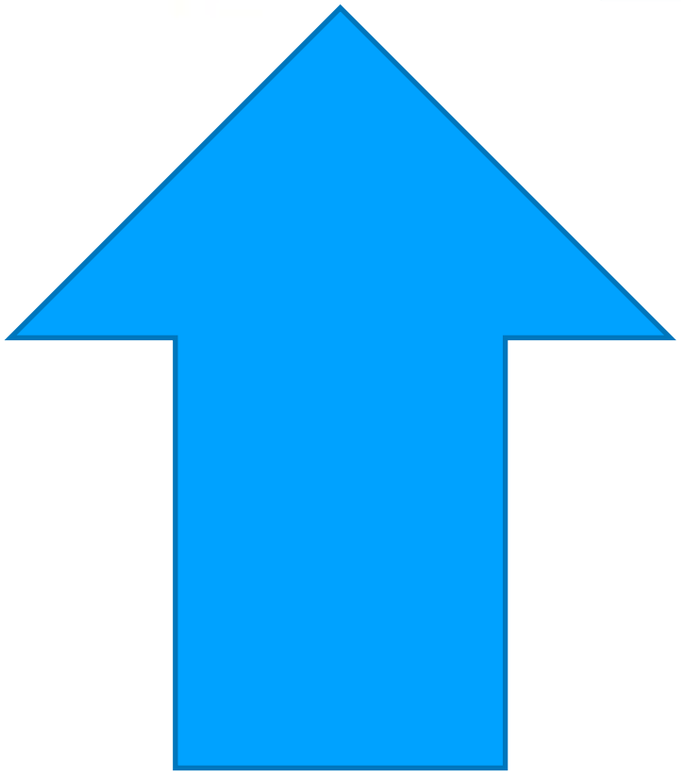
(1.795 nello stesso periodo 2017)

Ma nella realtà, gmail come dato di contatto…

Training of Lawyers on the European Data Protection Reform

#TRADATA

RESPONSABILE PER LA PROTEZIONE DATI: Avv.
email: **@gmail.com**, pec:



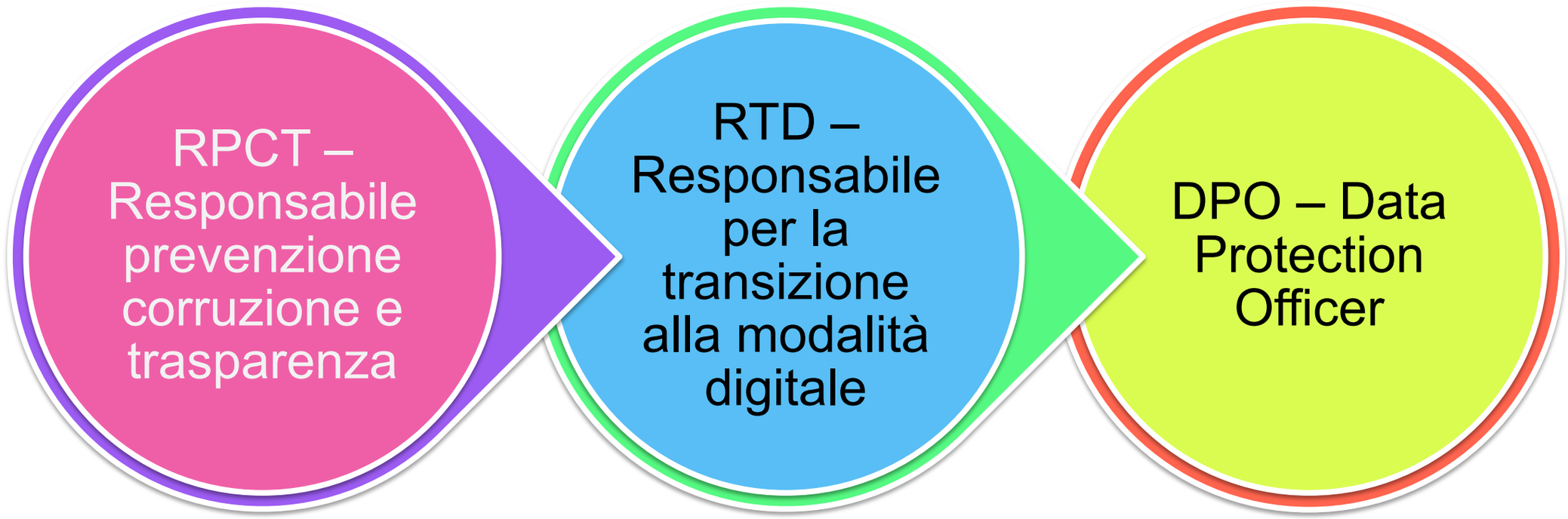
DPO pubblico: i bandi di gara

- Massimo ribasso e minor prezzo sono protagonisti indiscussi
- Data protection officer a 1000 €, o anche meno…
- Assenza di chiarezza nelle funzioni
- Previsione dell'attività di adeguamento unitamente alla funzione di DPO (con conseguenti profili di possibile conflitto d'interesse)

Il mancato coinvolgimento del DPO

- Nuovi trattamenti di dati (o modifiche significative) senza che il DPO venga coinvolto
- Assenza di consapevolezza dei vertici dell'ente (o dell'azienda)
- Mancanza di cooperazione nei controlli

Il DPO e le altre figure (settore pubblico)



Responsabilità del DPO?

Cosa è la sicurezza delle informazioni?

- **C - Confidenzialità**
- **I - Integrità**
- **A - Disponibilità**

Articolo 32 - Sicurezza del trattamento

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 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.

Articolo 32 - Sicurezza del trattamento

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. **Il titolare del trattamento e il responsabile del trattamento 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.

Alcuni punti fermi sulla sicurezza

Sogei
@SogeiUffStampa

Si invitano i Comuni a non fornire telefonicamente alcuna informazione sulle credenziali di accesso ai sistemi, tra cui #ANPR, a soggetti che si fingono “tecnici Sogei”.
Sogei fornisce supporto esclusivamente tramite i canali di contatto ufficiali. goo.gl/3BeSfK

sogei

Nota stampa

Si segnala che nei giorni scorsi “alcuni soggetti” hanno contattato telefonicamente dipendenti addetti ai servizi anagrafici di comuni italiani, presentandosi come tecnici Sogei al fine di ottenere credenziali di accesso a diversi sistemi tra cui quello dell'Anagrafe Nazionale Popolazione Residente (ANPR).

Tali persone **non sono dipendenti o collaboratori Sogei** e **non agiscono per conto dell'azienda**. Sogei infatti fornisce informazioni e supporto ai comuni per ANPR, esclusivamente tramite i canali di contatto ufficiali e in ogni caso non richiede password o altre credenziali ai dipendenti comunali.

Si invitano pertanto i comuni a non fornire alcuna informazione inerente le credenziali di accesso ai sistemi ad alcun soggetto e a denunciare l’accaduto all’autorità giudiziaria.

Roma, 23 novembre 2018

Complicità della vittima…

As described in chapter 5, the human element is one of the most common attack vectors used by threat agents. According to a recent survey[333], some of the most common information that people unknowingly make available online and can be abused are:

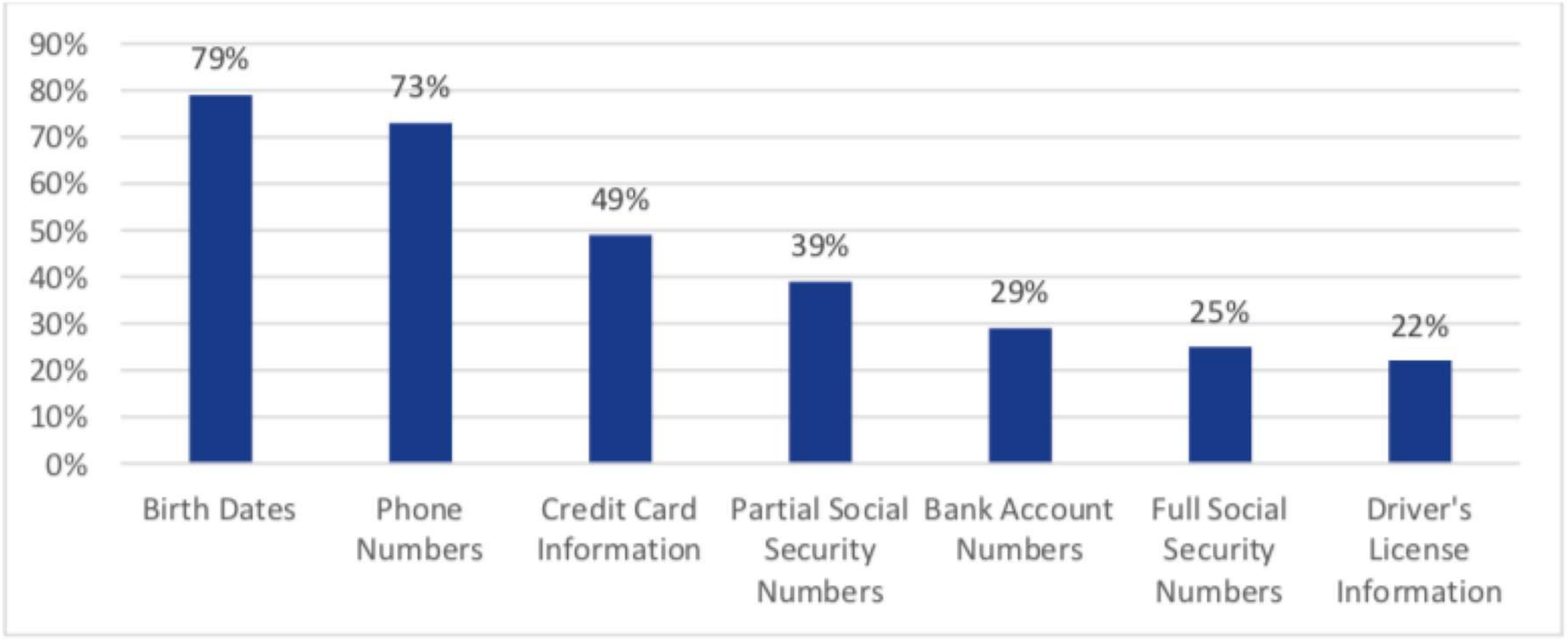


Image from ENISA Threat Landscape Report 2017 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

MISURE TECNICHE (no numero chiuso)

- **pseudonimizzazione** e **cifratura** dei dati personali (art. 32)
- capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità [**CIA**] (art. 32)
- capacità di assicurare su base permanente la **resilienza** dei sistemi e dei servizi di trattamento (art. 32)
- capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedura per **testare, verificare e valutare regolarmente** l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (art. 32)
- Privacy-By-Default - minimizzazione (art. 25)
- Privacy-By-Design

MISURE ORGANIZZATIVE (no numero chiuso)

- Scelta corretta dei responsabili del trattamento - art. 28
- Formazione (di tutti i soggetti autorizzati al trattamento)
- Designazione dei rappresentanti dei titolari extra UE - art. 27
- Nomina del responsabile della protezione dei dati (DPO) - art. 37
- Redazione di policy specifiche
- Eventuale adesione a codici di condotta
- Eventuale certificazione

Data Breach

Sicuro!

Training of Lawyers on the European Data Protection Reform

#TRADATA

Sicuro?

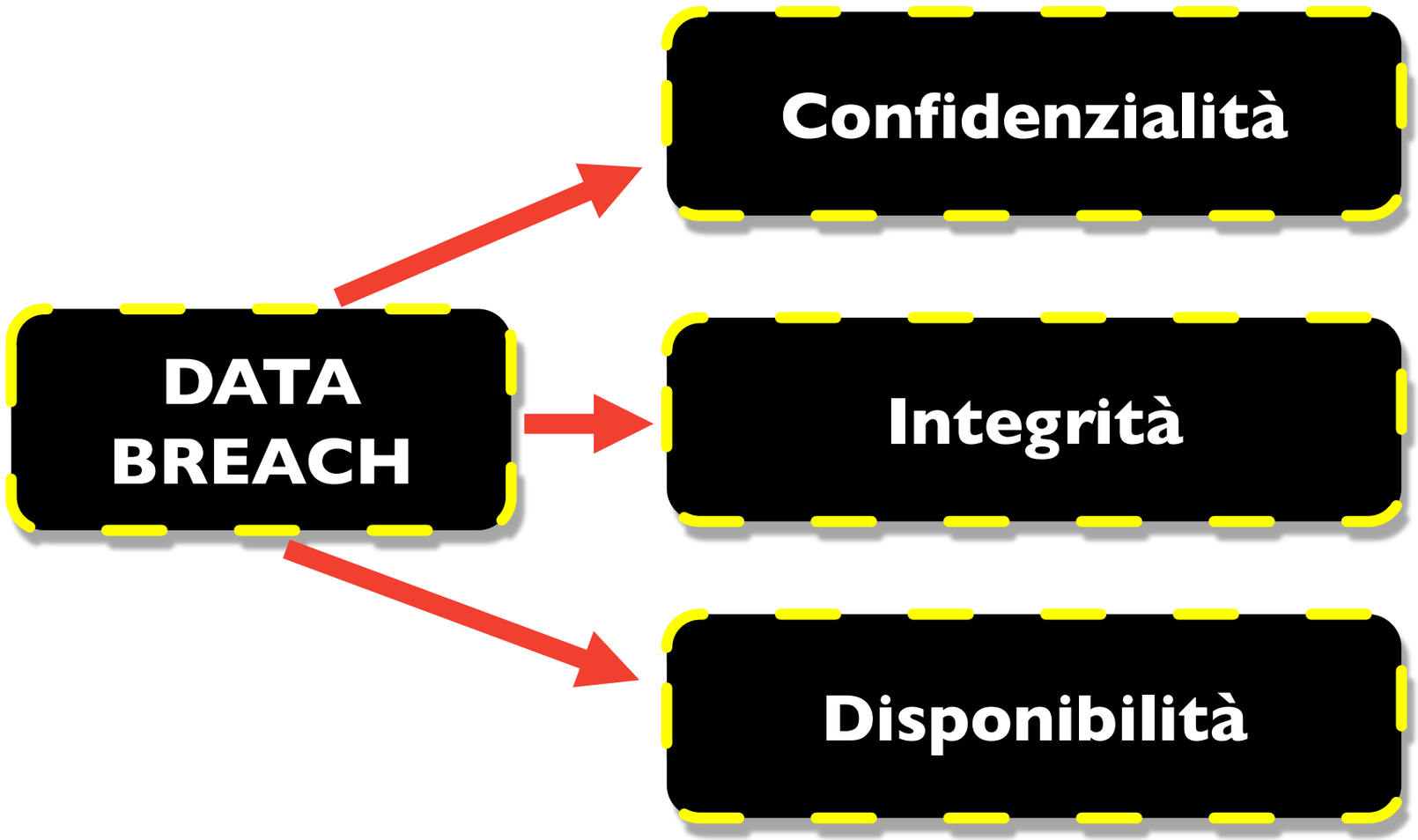

Technology
Want the best of Wi
ails
he security flaws at the hea
he Panama Papers
MATT BURGESS and
MES TEMPERTON
nesday 6 April 2016
A massive leak from Panama City-based law firm M
dealings of scores of world leaders and celebri
Credit RODRIGO ARANGUA/AFP/Getty Images
The front-end


tg24
HOME VIDEO FOTO CRONACA ED. LOCALI
UN PIAT
CRONACA
20
Attacco hacker ai tribunali, lo Stato: "Cambiate password della Pec"


Search jobs
Sign in
Search
The Guard
Culture
Lifestyle
More
Syndicate B2B
ways data breach: what to do
been affected
nts have been compromised to future bookings
stomer data stolen from its website
mpensate customers after data breach
nage to lift the details of BA customers?

Data breach…

quali data breach?



Definizione di Data Breach (art. 4)

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito

- la **distruzione**,
- la **perdita**,
- la **modifica**,
- la **divulgazione non autorizzata** o
- l'**accesso [non autorizzato]** ai dati personali trasmessi, conservati o comunque trattati

le cause frequenti dei data breach

- ***Errore umano***
  - *Errori di configurazione*
  - *Errori nella gestione*
  - *Formattazione e dismissione*
  - *Compromissione dei backup*
  - *Danni da liquidi*
  - *Imprudenze e negligenze*
- ***Attacchi***
  - *Accessi abusivi esterni/insiders*
  - *Leak dei dati*
  - *Virus & Malware*
  - *Social engineering*
  - *Furti e danneggiamenti*
- ***Danni e hardware***
- ***Fornitura di energia***
- ***Eventi naturali***
  - *roditori, funghi…*
  - *incendi, allagamenti etc*
- ***Obsolescenza hardware e software***

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username pwned?

269	4,868,606,237	64,429	70,991,519
pwned websites	pwned accounts	pastes	paste accounts

www.haveibeenpwned.com

Top 10 breaches

accounts

593,427,119 Exploit.In accounts

457,962,538 Anti Public Combo List accounts

Data breach GDPR (artt. 33-34)

DATA BREACH

Rischio per diritti e libertà degli interessati

Improbabile rischio per diritti e libertà degli interessati?

Nessuna Segnalazione (l'evento va comunque documentato)

Garante (notifica)

Probabile rischio elevato per diritti e libertà degli interessati?

Interessati (comunicazione)

quando è improbabile il rischio derivante da data breach?

- *if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly **encrypted personal data** may not need to be notified to the supervisory authority (WP29)*

Art. 33 GDPR

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

Questo ultimo obbligo va **specificato nell'accordo negoziale con il data processor**, ex art. 28, comma 3

[…] Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

*f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli **articoli da 32 a 36**, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;*

Art. 33 GDPR

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

5. Il titolare del trattamento **documenta qualsiasi violazione dei dati personali**, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente **[shall enable]** all'autorità di controllo di verificare il rispetto del presente articolo.

quando non è dovuta la comunicazione all'interessato

a) **il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate** ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la **cifratura**;

b) il titolare del trattamento 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;

c) **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.

I dati del Garante

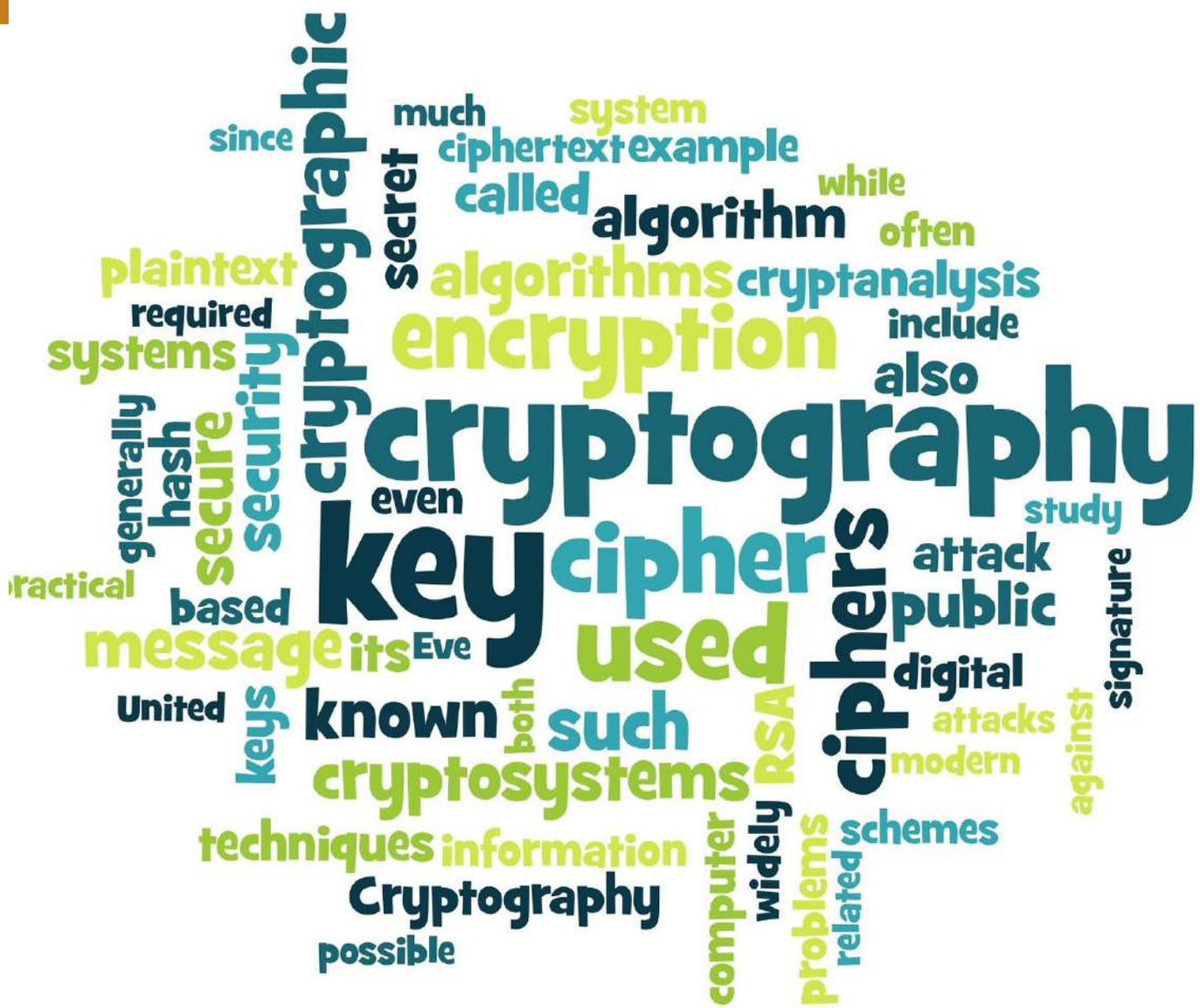
Notificazioni di Data Breach **305**

Contatti con l'URP **circa 7.200**

(circa 4.400 nello stesso periodo 2017)

Guidelines on personal data breach notification

For the European Union Institutions and Bodies



Data breach: cosa fare in pratica?

- Applicare il principio di minimizzazione (in tutte le sue declinazioni)
- Cifrare i dispositivi e le periferiche
- Cifrare le comunicazioni
- Verificare periodicamente tutte le misure di sicurezza
- Selezionare accuratamente i responsabili ex art. 28 GDPR
- Creare il registro delle violazioni
- Redigere una procedura snella per la gestione del data breach

- Ma, soprattutto, ricordarsi che …

Human error wins… e quindi formazione e consapevolezza sono fondamentali


Compliant you must be. Protected your data.
When 900 years old you reach, you may understand the true power of GDPR
imgflip.com

Grazie

per l'attenzione

TRADATA

TRAINING OF LAWYERS ON THE EUROPEAN UNION'S DATA PROTECTION REFORM

D.ssa Laura Ferola

Training of Lawyers on the European Data Protection Reform

#TRADATA

Training of Lawyers on the EU Data Protection Reform (TRADATA)

The project is co-financed with the support of the European Union's Rights, Equality and Citizenship programme

1. **BREVE RICOSTRUZIONE DELL'EVOLUZIONE NORMATIVA**

2. **ISTITUZIONE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI: LE FONTI**

3. **PRINCIPI FONDAMENTALI**

4. **LE COMPETENZE**

5. **L'AZIONE TRANSNAZIONALE**

#TRADATA

Training of Lawyers on the European Data Protection Reform

Verso il futuro

- **cyberspazio + globalizzazione**

- **web: spazio virtuale senza frontiere**

- **obsolescenza dei sistemi giuridici tradizionali** (strumenti e regole di diritto che si arrestano ai confini nazionali o europei)

- esigenza di **nuove forme di tutela dell'identità personale**

- **necessari strumenti sovranazionali**

nuovi mondi

nuove fonti

la fluttuazione del diritto

- **Regolamento** (UE) 2016/679: **protezione delle persone fisiche con riguardo al trattamento e alla circolazione dei dati personali**

- **Direttiva** (UE) 2016/680: trattamento di dati personali a fini di prevenzione, accertamento di **reati** o esecuzione di **sanzioni penali**

Le Fonti

* **Carta dei diritti fondamentali dell'UE**

* **Convenzione CoE 108/1981 e Protocolli addizionali *(2001 e 2018)***

* **Direttiva (UE) 2016/680 = *d.lgs. n. 51/2018***

* **Regolamento (UE) 2016/679**

* **Codice in materia di protezione dei dati personali *(d.lgs. n. 196/2003 modificato dal d.gs. n. 101/2018) - già l. n. 675/1995***

Autorità di controllo

Regolamento
(artt. 51- 56)

* *indipendenza*
* *istituzione*
* *competenza*

Codice
(artt. 2-bis, 153, 155, 156)

* *Garante per la protezione dei dati personali*
* *composizione*
* *Ufficio*

Compiti e Poteri

Regolamento
(artt. 55-62, 83)

* ***competenza territoriale***
* ***compiti di sorveglianza e impulso***
* ***poteri di indagine, correttivi e sanzionatori, autorizzativi e consultivi***

Codice
(artt. 154, 154-bis, 157-166)

* ***tutele e garanzie***
* ***controllo e assistenza settoriali***
* ***promozione della conoscenza***
* ***accertamenti e sanzioni***

Meccanismi di cooperazione e di coerenza

(Regolamento: cons. 124 e ss.; artt. 56-76)

trattamenti transfrontalieri

DPA interessate

DPA capofila

Comitato europeo per la protezione dati

- progetto di decisione
- informazioni utili
- assistenza reciproca e operazioni congiunte
- obiezioni
- composizione delle controversie

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

#TRADATA

Training of Lawyers on the European Data Protection Reform

Piazza Venezia, 11 - 00186 Roma

garante@garanteprivacy.it

www.garanteprivacy.it

tel.: 06.69677.1 - fax: 06.69677.3785

Ufficio relazioni con il pubblico

urp@garanteprivacy.it

(lunedì - venerdì ore 10-13)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Grazie per l'attenzione

#TRADATA

Training of Lawyers on the European Data Protection Reform

#TRADATA

STUDIO PREVITI
ASSOCIAZIONE PROFESSIONALE

Training of Lawyers on the European Union's Data Protection Reform

Roma, 12.12.2018

Sviluppi delle norme nazionali sulla protezione dei dati

(D.Lgs 196/2003 e ss.mm.ii. D.Lgs 101/2018)

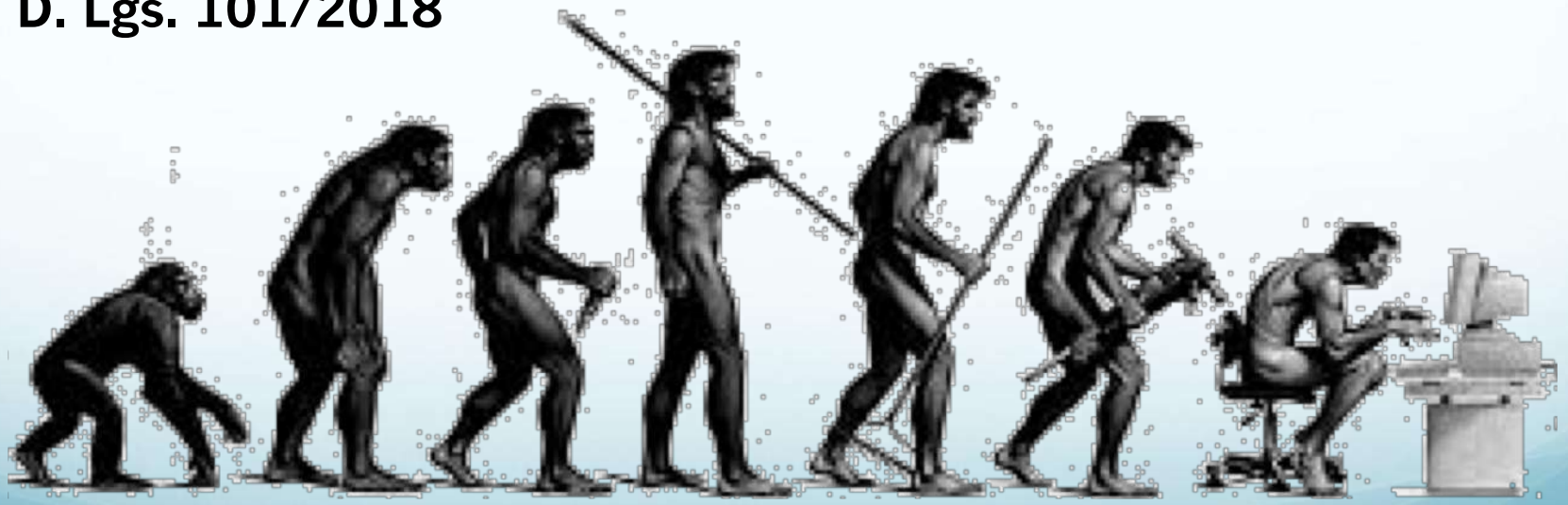
Vincenzo Colarocco, Avvocato del Foro di Roma

L'evoluzione della *privacy*

- ***Right to be alone***
- **Direttiva 95/46/EC**
- **D. Lgs. 196/03 (Codice della *privacy*)**
- **Regolamento Europeo 679/2016**
- **D. Lgs. 101/2018**

#TRADATA

Training of Lawyers on the European Data Protection Reform



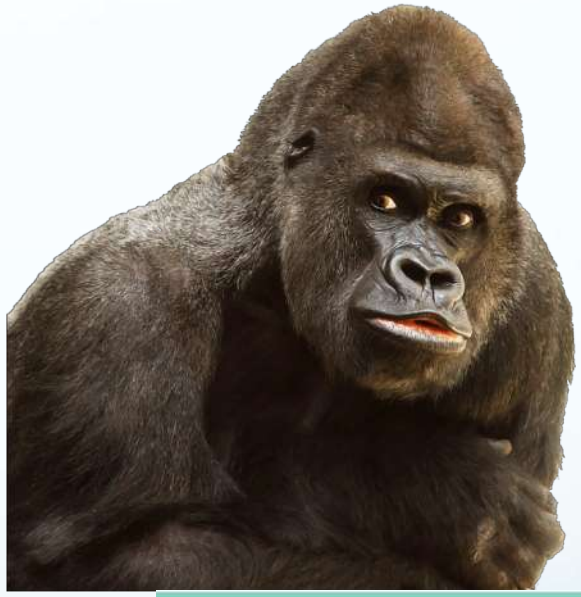
Di cosa parleremo

1) Evoluzione normativa

- D. Lgs. 196/03 (Codice della *privacy*)
- Regolamento Europeo 679/2016
- D. Lgs. 101/2018

2) Focus: il dato biometrico

3) Focus: marketing diretto



#TRADATA

Training of Lawyers on the European Data Protection Reform

Il Regolamento Europeo in materia di protezione dei dati personali 2016/679

Avv. Vincenzo Colarocco

@colarocco

STUDIO ASSOCIAZIONE PREVITI PROFESSIONALE

Cosa è successo con il «famoso» 25 maggio?

- **Il Regolamento n. 679/2016** è divenuto obbligatorio
- **La Direttiva n. 46/1995** è stata abrogata
- **Le Autorizzazioni generali del Garante** sono decadute
- **I Provvedimenti dell'Autorità Garante** non sono decaduti e non decadranno sino a quando non saranno modificati, abrogati, sostituiti
- **Gli Accordi Internazionali** sul trasferimento dei dati non sono decaduti e non decadranno sino a quando non saranno modificati, abrogati, sostituiti
- **Le Decisioni della Commissione UE** non sono decaduti e non decadranno sino a quando non saranno modificati, abrogati, sostituiti

Recap delle novità

- *Data Protection Officer*
- Registro dei trattamenti
- Valutazione d'impatto adozione di misure tecniche e organizzative adeguate
- *Accountability* del titolare
- *Data breach*
- Portabilità dei dati
- Conservazione dei dati
- *Privacy by design* e *privacy by default*
- Entità delle sanzioni
- Certificazione dei trattamenti

#TRADATA

Training of Lawyers on the European Data Protection Reform

Invariati o variati marginalmente

- Definizione di trattamento
- Definizione di dato personale
- Principi relativi al trattamento di dati
- Liceità del trattamento
- Obbligo di informativa
- Obbligo di consenso
- Soggetti che effettuano il trattamento (salvo incaricati e DPO)
- Protezione delle sole persone fisiche
- Responsabili esterni e fornitori

Il «nuovo» Codice della Privacy

In data **10 agosto 2018** è stato pubblicato in Gazzetta Ufficiale il decreto di armonizzazione n. 101.

Il decreto ha provveduto ad armonizzare le disposizioni del D. Lgs. n. 196/2003 («Codice Privacy») alle nuove prescrizioni del GDPR

In vigore dal 19 settembre 2018

Armonizzazione del Codice Privacy al GDPR

Art. 22 D. Lgs. 101/2018

«Il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra Stati membri ai sensi dell'articolo 1, paragrafo 3, del Regolamento (UE) 2016/679».

Art. 2 Codice Privacy riformato

«Il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento».

EFFETTI:

Supremazia della normativa Ue su quella nazionale

Le disposizioni italiane sono legittime se:

1. Rientrano nelle **materie** rimesse dal GDPR al legislatore nazionale;
2. Il contenuto è **conforme** alle disposizioni del GDPR;
3. Sono **interpretate** e **applicate** nel rispetto del Regolamento.

Il GDPR parametro di legittimità della normativa nazionale

Interpretazione, applicazione, risoluzione di **antinomie** tra norme in contrasto con le disposizioni contenute nel GDPR saranno illegittime.

Esiste una responsabilità in capo a Garante e Autorità giudiziaria

Le integrazioni in concreto

- Precisazioni in tema di **dati particolari**: genetici, biometrici, relativi alla salute e a condanne;
- **Limitazione dei diritti degli interessati**, ad integrazione dei casi già presenti nel Regolamento (art. 23), in determinate ipotesi;
- Attribuzione di funzioni e compiti a **soggetti designati**;
- Il consenso dei **minori italiani** sin dall'età dei 14 anni;

Le integrazioni in concreto

- Nei casi di ricezione dei **curricula spontaneamente trasmessi dai candidati**, al fine della instaurazione di un rapporto di lavoro, l'informativa deve esser fornita al momento del primo contatto utile. Il consenso al trattamento dei dati personali non è dovuto;

- La gestione dei diritti riguardanti **le persone decedute**;

- **Regime sanzionatorio**: criteri per la determinazione delle sanzioni amministrative e illeciti penali.

Cosa dovrà fare il Garante?

FUNZIONI AMMINISTRATIVE

- **Attività provvedimentale:**

1. Adozione di provvedimenti di carattere generale per i trattamenti che presentano rischi elevati (art. 2 quinquiesdecies);
2. Approvazione delle regole deontologiche di cui all'art. 2 quater (art. 154);

- **Attività consultiva:**

1. Formulazione di una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla privacy da trasmettere al Parlamento e al Governo (art. 154);
2. A seguito di una proposta di atto legislativo, formulazione di un parere nei termini di 45 giorni decorso il quale potrà procedersi senza (art. 154);

Cosa dovrà fare il Garante?

FUNZIONI AMMINISTRATIVE

- **Attività di vigilanza** (anche ispettiva):

richiesta di informazioni ed esibizioni documenti al titolare o al responsabile del trattamento (art. 157), anche con acceso a banche dati.

#TRADATA

Training of Lawyers on the European Data Protection Reform

Cosa dovrà fare il Garante?

FUNZIONI NORMATIVE

1. **Linee guida** di indirizzo

2. **Misure** di garanzia per il trattamento dei dati genetici, biometrici e sanitari.

#TRADATA

Training of Lawyers on the European Data Protection Reform

Cosa dovrà fare il Garante?

FUNZIONI CONTENZIOSE

Art. 140 *bis*

«Qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, l'interessato può proporre **reclamo al Garante** o **ricorso dinanzi all'autorità giudiziaria**.
Il reclamo al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.
La presentazione del reclamo al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto, salvo quanto previsto dall'articolo 10, comma 4, del decreto legislativo 1° settembre 2011, n. 150».

FOCUS: Dato Biometrico

DATO BIOMETRICO

- PROVVEDIMENTI AUTORITA' GARANTE
- REGOLAMENTO EUROPEO 679/16 (GDPR)
- CODICE PRIVACY

Dato Biometrico & Garante Privacy

Provvedimento a carattere generale in materia di biometria del 12 novembre 2014

Viene meno l'obbligo di richiesta di verifica preliminare, se:

I soggetti pubblici e privati **si atterranno ai limiti e alle rigorose misure di sicurezza** individuati dal Garante Privacy.

Il Provvedimento

L'Autorità ha:

- individuato specifici casi in cui **non sarà più necessario effettuare un interpello preventivo**
- imposto ai titolari di trattamenti di dati biometrici di comunicare **entro 24 ore** dal fatto, qualsiasi **incidente** informatico o violazione di dati che riguardi dati biometrici
- emanato **Linee Guida** nelle quali vengono analizzati i vari tipi di trattamento biometrico esistenti, inclusi quelli per i quali **permane l'obbligo delle verifica preliminare**

Il Provvedimento

Il provvedimento di carattere prescrittivo dispone come **debbano essere comunque rispettate** le misure e gli accorgimenti di carattere tecnico, organizzativo e procedurale stabiliti dal Garante:

- fornire sempre un'adeguata **informativa** agli interessati
- acquisire il **consenso**, ove richiesto
- se necessario effettuare la **notificazione** ai sensi degli artt. 37, comma 1, lett. a), e 38, del Codice se necessaria

Il Provvedimento

I trattamenti **«esentati»** dalla verifica preliminare sono quelli in cui i dati biometrici sono utilizzati:

- nell'ambito di procedure di **autenticazione informatica**
- per il **controllo di accesso fisico ad aree "sensibili"** dei soggetti addetti e per l'utilizzo di apparati e macchinari pericolosi
- per **scopi "facilitativi"** mediante l'uso dell'impronta digitale o della topografia della mano
- per la **sottoscrizione di documenti informatici**

Dato Biometrico & GDPR: cambia il quadro normativo

- ✓Considerando 51, 89, 91
- ✓Articolo 4, punto 14
- ✓Articolo 9 par. 4
- ✓Articolo 35
- ✓Articolo 36

Codice Privacy

- ✓Articolo 2 *sexies*
- ✓Articolo 2 *septies*

Dato Biometrico & GDPR

Considerando 51

«Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di **dati biometrici** soltanto quando saranno trattate attraverso un **dispositivo tecnico specifico** che consente **l'identificazione univoca** o l'autenticazione di una persona fisica».

Considerando 89

«È pertanto opportuno **abolire** tali **obblighi generali e indiscriminati di notifica** e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità».

Dato Biometrico & GDPR

Considerando 91

«È opportuno altresì effettuare una **valutazione d'impatto** sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, **dati biometrici** o dati relativi a condanne penali e reati o a connesse misure di sicurezza».

Dato Biometrico & GDPR

Il **GDPR** (art. 4 punto 14) definisce i dati biometrici come:

«i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano **l'identificazione univoca**, quali **l'immagine facciale** o i **dati dattiloscopici**».

Dato Biometrico & GDPR

È ***vietato trattare dati biometrici*** (art. 9) intesi a identificare in modo univoco una persona fisica, ***salvo*** che:

- l'interessato ha prestato il proprio ***consenso*** esplicito
- Il trattamento 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
- il trattamento è necessario per tutelare un ***interesse vitale***
- necessari per motivi di ***interesse pubblico rilevante***

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Dato Biometrico & Codice Privacy

Art. 2 *sexies*

21 casistiche di interesse pubblico tra cui:

- compiti del **servizio sanitario nazionale** e dei soggetti operanti in ambito sanitario, nonche' compiti di igiene e **sicurezza sui luoghi di lavoro** e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumita' fisica;

- instaurazione, gestione ed estinzione, di **rapporti di lavoro** di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene **e sicurezza del lavoro** o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva .

Dato Biometrico & Codice Privacy

Art. 2 *septies*

I dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza delle condizioni di legittimità del GDPR ed **in conformità alle misure di garanzia disposte dal Garante**, nel rispetto di quanto previsto dal presente articolo

Il provvedimento che stabilisce le **misure di garanzia è**

- adottato con cadenza **almeno biennale**
- sottoposto a **consultazione pubblica** per un periodo non inferiore a sessanta giorni
- adottato tenendo conto **dell'evoluzione scientifica** e **tecnologica** nel settore oggetto delle misure e dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

Dato Biometrico & Codice Privacy

Art. 2 *septies*

Le misure di garanzia individuano le **misure di sicurezza**, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalita' per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonche' le eventuali altre misure necessarie a garantire i diritti degli interessati.

L'utilizzo dei dati biometrici è considerato una **misura di sicurezza** con riguardo alle procedure di **accesso fisico e logico** ai dati da parte dei soggetti autorizzati, nel **rispetto delle misure di garanzia** di cui al presente articolo

I dati genetici, biometrici e sanitari **non possono essere diffusi.**

FOCUS: Comunicazioni Indesiderate

Marketing diretto e Legittimo Interesse

Cosa si intende per legittimo interesse?

Considerando 47

«Può essere considerato **legittimo interesse** trattare dati personali per finalità di **marketing diretto**».

Considerando 70

«Qualora i dati personali siano trattati per finalità di **marketing diretto**, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di **opporsi** a tale trattamento, con riguardo sia a quello iniziale che a quello ulteriore, **compresa la profilazione** nella misura in cui sia **connessa a tale marketing diretto.** Tale diritto dovrebbe essere esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione».

Cosa accade con il D. Lgs. 101/2018

Art. 140 (Abrogato)

«Il Garante promuove, ai sensi dell'articolo 12, la **sottoscrizione di un codice di deontologia** e di buona condotta per il trattamento dei dati personali effettuato a fini di invio di **materiale pubblicitario** o **di vendita diretta**, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale, prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni»

Art. 130 (Parzialmente modificato)

«1…l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il **consenso** del contraente o utente».

Questione n. 1

È possibile pensare ad un'**antinomia** tra norme?

Art. 6 lett. f) GDPR ⟷ **Art. 130 Cod.Privacy**

Se sì, come **risolverla**?

Come risolvere il presunto conflitto?

Criterio gerarchico - Primazia del diritto comunitario sul diritto interno:

o

Criterio della specialità:

In questo caso verrebbero considerate due (o tre) fonti: il **GDPR**, la **Direttiva ePrivacy** e il **Regolamento ePrivacy**. Il conflitto sarebbe risolto dallo stesso art. **95** del GDPR

«Il presente **regolamento non impone obblighi supplementari alle persone fisiche o giuridiche** in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE».

Ragioni

Il rapporto tra **Direttiva ePrivacy** e il **GDPR** è di complementarietà

Mira ad assicurare la **riservatezza** e la **sicurezza** delle comunicazioni elettroniche nonché l'integrità delle informazioni

Mira alla tutela dei **diritti** e delle **libertà fondamentali** non specificamente disciplinati dalle disposizioni della Direttiva ePrivacy

Questione n. 2

L'utilizzo della base giuridica del **legittimo interesse** rappresenta una scelta che deve essere valutata **attentamente** perché potrebbe avere ampie ricadute di carattere operativo.

L.I.A.

Ratio

effettuare un bilanciamento tra gli interessi del titolare o di terzi con i diritti e le libertà fondamentali degli interessati

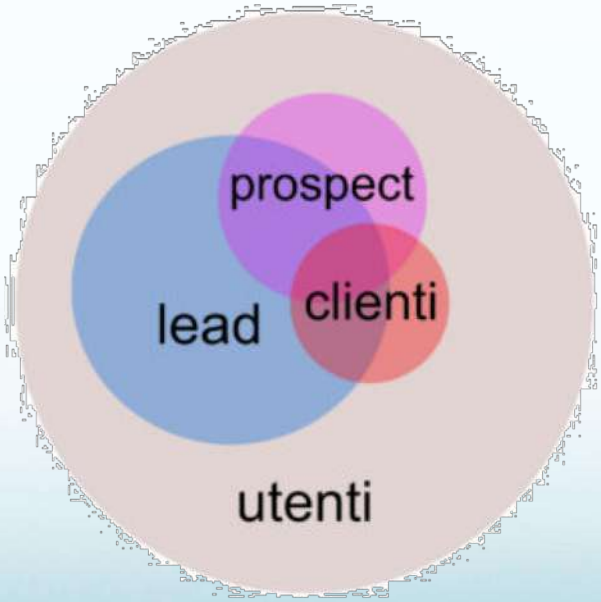
Articolo 130 comma 4 Codice Privacy

«...se il titolare del trattamento utilizza, a **fini di vendita diretta** di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può **non** richiedere **il consenso** dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni...»

Clienti Prospect e L.I.A.

Se, a seguito di una L.I.A., per il trattamento dei dati dei clienti *prospect* sussista un legittimo interesse

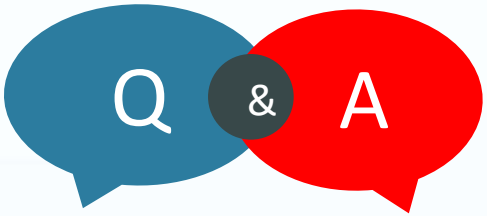
Art. 130 comma 4 Codice Privacy?



Proposta di Regolamento ePrivacy

L'**art. 16** sembra confermare quanto finora esposto, infatti:

«Le persone fisiche o giuridiche possono avvalersi dei servizi di comunicazione elettronica al fine di inviare comunicazioni di commercializzazione diretta a utenti finali aventi natura di persone fisiche che hanno espresso il loro consenso».



THANKS FOR LISTENING

WE'LL BE ANSWERING QUESTIONS NOW

#TRADATA

Training of Lawyers on the European Data Protection Reform

GRAZIE PER L'ATTENZIONE

Avv. Vincenzo Colarocco

vincenzocolarocco@previti.it