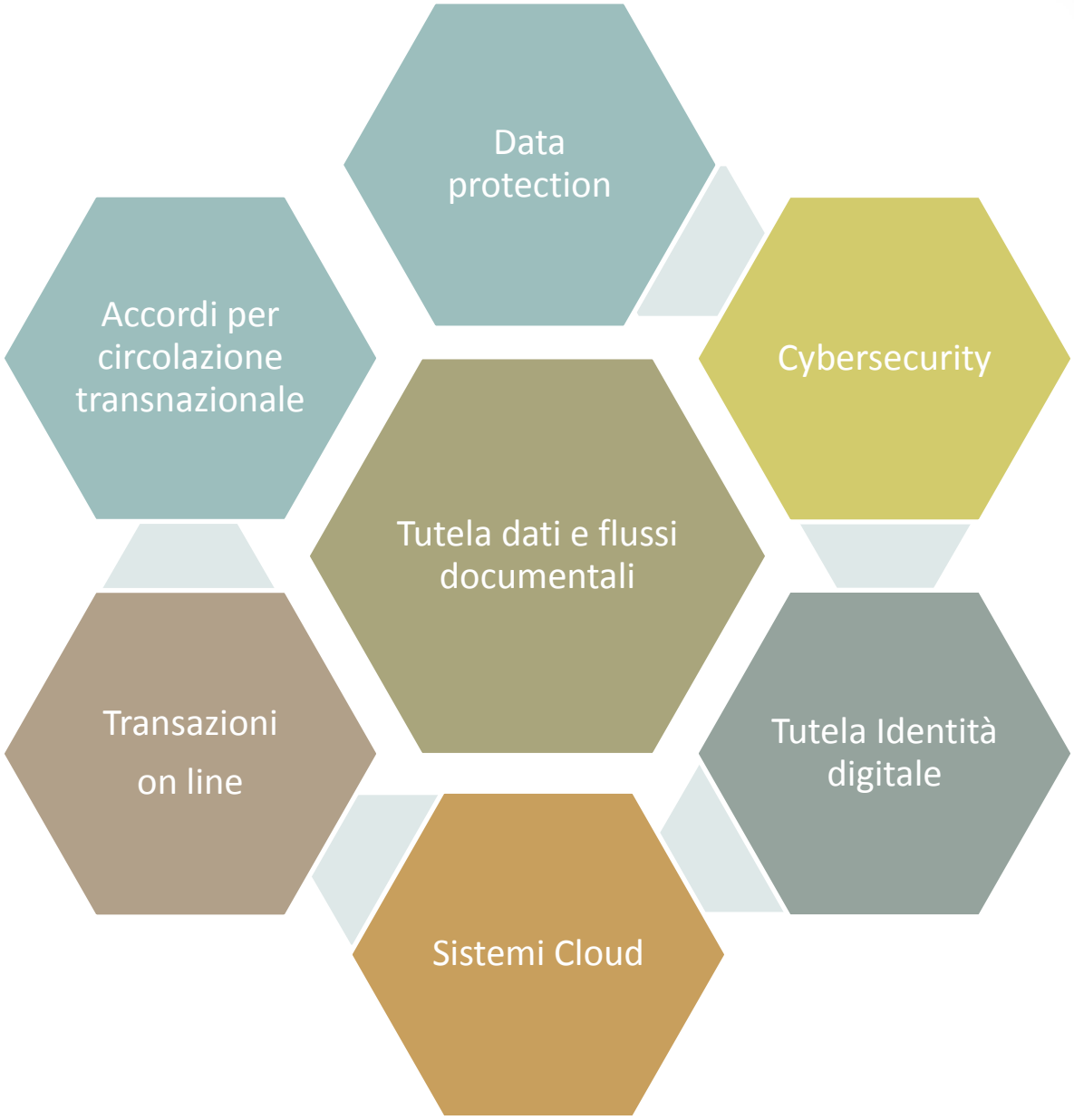
Prof. ssa A. Busacca
Università Mediterranea
di Reggio Calabria

Data protection

prospettive e novità
tra GDPR e strumenti rimediali "interni"


Data protection
Accordi per circolazione transnazionale
Cybersecurity
Tutela dati e flussi documentali
Transazioni on line
Tutela Identità digitale
Sistemi Cloud

Security Incidents

- Attacchi per mezzo di applicazioni on line (*malaware*)
- Intrusioni nel sistema dei pagamenti elettronici
- Utilizzo abusivo di informazioni risarvate
- Errori e negligenze nella custodia
- Furto, smarrimento, perdita dei dati
- Crimeware
- Skimming
- Spionaggio informatico
- Interruzione di servizio (es. gaming o fin-tech)

Privacy e Data Protection

- *Matrice giurisprudenziale*
- *Contenuto «negativo»*
- *Matrice normativa sovranazionale*
- *Contenuto «positivo»*
- *Art.2050 c.c.*

Evoluzione della disciplina europea

- Direttiva 1995/46 — standard e disciplina comunitaria in materia di trattamento dati
- Direttiva 1997/66 — trattamento dati e tutela della vita privata nel settore delle telecomunicazioni
- Direttiva 2002/58 — trattamento dati e tutela della vita privata nel settore delle comunicazioni elettroniche
- Direttiva 2009/136 — e-privacy (cookie law)

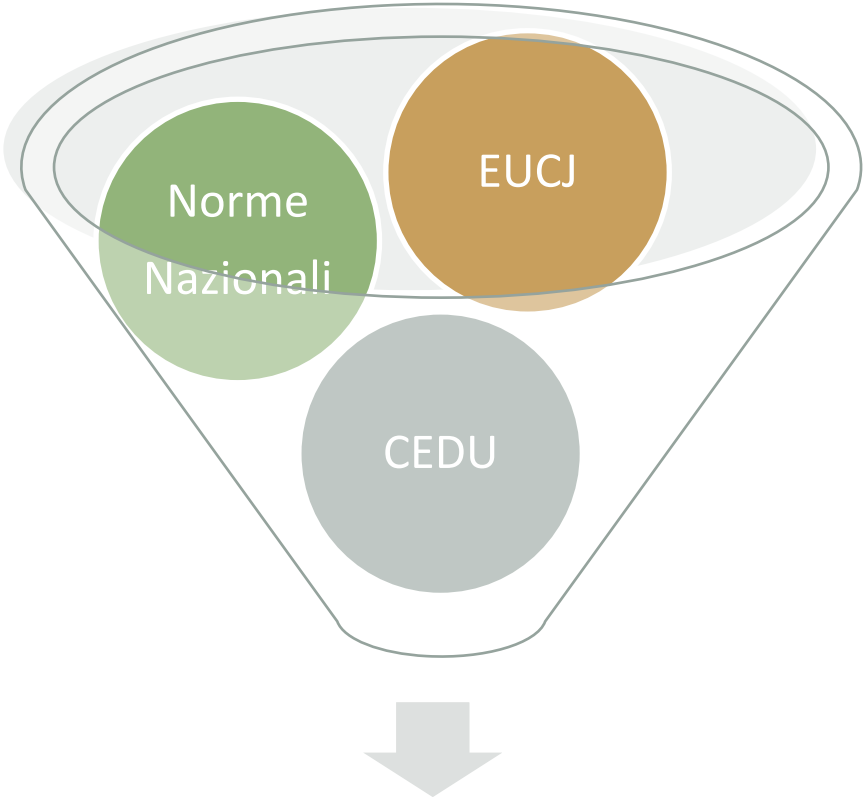
Regolamento (CE) n. 45/2001

concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati

European Court of Justice

- Digital Right Ireland *(8 aprile 2014, C-239/12)*
- Google Spain *(13 maggio 2014, C-131/12)*
- Scherms *(6 ottobre 2015, C-362/14)*

GENERAL DATA PROTECTION REGULATION



Disciplina unitaria

..tra novità e continuità...

Rafforzamento

Unificazione

Rinvio al legislatore nazionale per specifiche categorie di trattamenti

↓

Livello di protezione «equivalente»

Misure → *giuridiche*, *tecniche*, *organizzative*

Principali innovazioni

- Ambito territoriale di applicazione
- Ambito materiale di applicazione

- Principio
- Risk-based approach

- DPO
- Procedure in caso di Data Breach

Ambito di applicazione territoriale

Stabilimento

Esercizio effettivo e reale di una attività mediante una organizzazione stabile

Cfr. Google Spain; Weltimmo

Targeting

offerta di beni e servizi, indipendentemente dall'obbligtorietà di un pagamento

monitoraggio dei comportamenti degli interessati

Ambito di applicazione materiale

Art.2 c.IV

Il presente regolamento **non pregiudica** pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva

Categorie particolari di dati

Art. 9 c. I

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati **genetici**, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi **alla salute o alla vita sessuale o all'orientamento sessuale** della persona

Eccezioni…

Art. 9 comma II prevede 10 ipotesi sottratte al generale divieto del comma I

….nell'interesse dell'interessato

a) Consenso
b) Dati resi manifestamente pubblici dall'interessato
c) Tutela dell'interesse vitale dell'interessato (in stato di incapacità)

….nell'interesse del titolare

d) Assolvere obblighi ed esercitare diritti del titolare

e) Trattamento da parte di associazione o fondazione o altro organismo senza scopo di lucro

…per interessi superiori o superindividuali

f) Esigenze di giustizia

g) Esigenze legate alla salute

h) Esigenze di interesse pubblico

i) Esigenze di interesse pubblico nel settore della sanità

j) Esigenze di carattere storico, ricerca scientifica o rilevazione statistica

Trattamenti sottratti al Regolamento

A)effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

B)effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

C)effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico

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 e la prevenzione delle stesse

Ambito di applicazione materiale

Art. 2 c.I

Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di **dati personali** e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Art. 4 c.I, lett. a)

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

household exclusion provision

Portata generale?

Come comportarsi con i Social Network Sites?

Cfr. considerando n.18

Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi **senza una connessione** con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere **la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività**. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico

Cfr. altresì art.2 c.IV Il Regolamento non pregiudica l'applicabilità della Direttiva 2000/31 in materia di responsabilità per il prestatore di servizi

«Trattamento»

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, *la strutturazione*, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, *l'uso*, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, *la limitazione*, la cancellazione o la distruzione

Diritti dell'interessato

Artt. 12, 13,14

Informazioni su

- Origine dei dati
- Identità e contatti del titolare e del responsabile
- Portabilità e restrizioni
- Tempi e modalità di conservazione
- Diritto ad adire l'autorità di controllo competente
- Legittimo interesse perseguito (** art.6, comma I, lett.f)

- Pseudonomizzazione
- Portabilità
- Limitazione
- Cancellazione /oblio

Diritti «nuovi»???

dall'approccio riparatorio all'approccio di tipo preventivo….

- Privacy by design

art.25

- Privacy by default

Policy & procedure per garantire compliance, specialmente a fini di minimizzazione dei dati

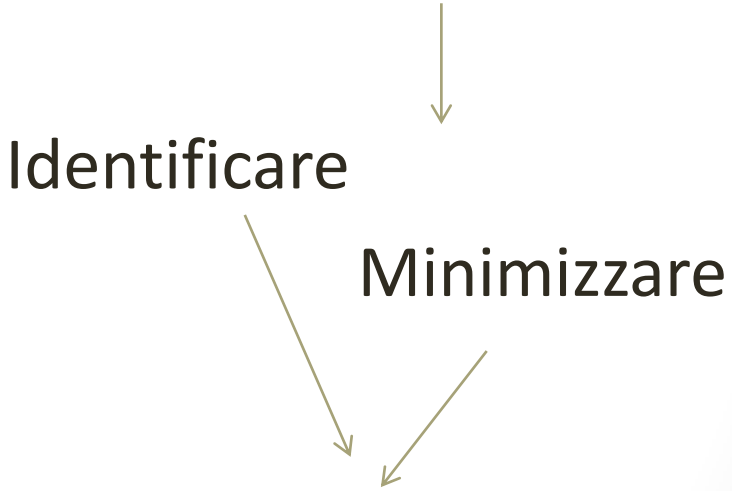
Valutazioni di impatto e *risk management*

Descrizione specifica dei trattamenti e delle finalità

Valutazione di proporzionalità del trattamento, dei rischi e delle misure di mitigazione

Audit

effettuata su aree specifiche



Art. 35

Quando un tipo di trattamento, allorché **prevede in particolare l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, **il titolare del trattamento effettua**, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Esempi di trattamento rischioso:

Profilazione, attività di trattamento dati sensibili su larga scala, sorveglianza di luogo accessibile al pubblico

Sicurezza del trattamento (art.32)

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;

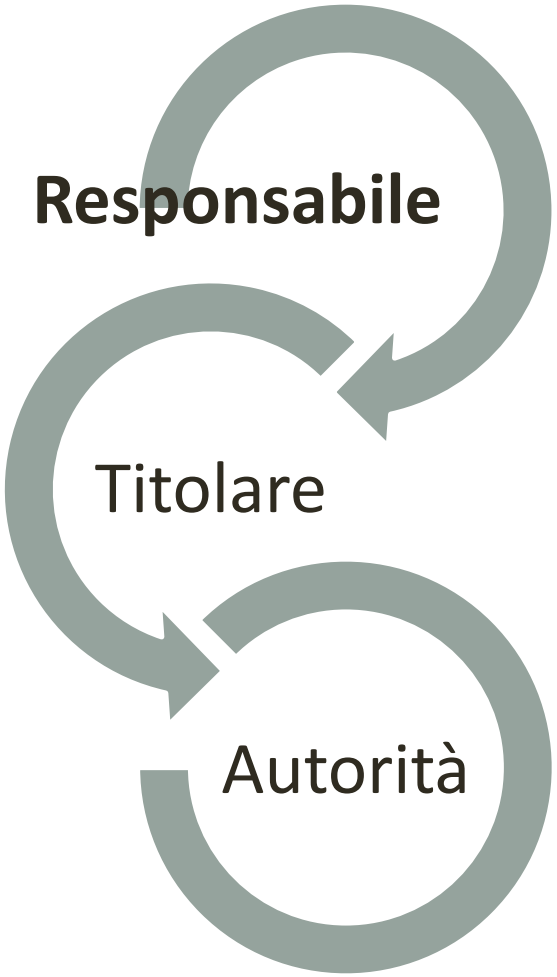
D)una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare **l'adeguato livello di sicurezza**, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, **conservati** o comunque trattati.

Cloud provider??

es. sanità, servizi finanziari, servizi di identificazione nell'immigrazione…..

Data Breach – art.33



Strumenti rimediali

- Tutela inibitoria
- Rimozione e distruzione dei contenuti
- Ripristino delle misure di sicurezza “interrotte” o danneggiate
- Risarcimento del danno

- Art. 58 GDPR

Strumenti rimediali

- Sanzione amministrativa

(art.83 GDPR)

- Art. 614 cpc ??
- Punitive damages ?

Verso la funzione afflittivo-sanzionatoria della responsabilità civile ?