UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Spgi | Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Spgi | Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali

Corso di laurea in Informatica

DIRITTO, INFORMATICA E SOCIETA'

Parte seconda, Prof. Andrea Sitzia

- Regolamento privacy: cos’è e perché?
- Accountability (cambio di mentalità)
- Le novità e la compliance

Scheda di sintesi a mero scopo divulgativo. Per un quadro completo della materia, si rimanda alla legislazione in tema di protezione dei dati personali e ai provvedimenti dell'Autorità.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Regolamento (UE) 2016/679

Una sintesi per aziende ed enti

Rispettare i diritti delle persone

Ogni trattamento deve fondarsi sul rispetto dei principi fissati nel Regolamento (artt. 5 e 6) e garantire agli interessati tutti i diritti previsti (artt. 13-22).

Individuare il rischio e svolgere una valutazione d'impatto

Ai titolari spetta il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, anche attraverso un apposito processo di valutazione che tenga conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) necessarie per mitigare tali rischi, eventualmente consultando il Garante alla luce di questa valutazione.

Redigere un registro dei trattamenti

Si tratta di uno strumento fondamentale per disporre di un quadro aggiornato dei trattamenti in essere. I contenuti minimi sono indicati all'art. 30 del Regolamento. Deve avere forma scritta, anche elettronica, e va esibito su richiesta al Garante.

Garantire la sicurezza dei dati

Il titolare e il responsabile del trattamento sono obbligati ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Nominare un Responsabile della protezione dei dati

La designazione (in vari casi obbligatoria) di un RPD riflette l'approccio responsabilizzante del Regolamento. Fra i suoi compiti rientrano la sensibilizzazione e formazione del personale, la sorveglianza sullo svolgimento della valutazione di impatto, la funzione di punto di contatto per gli interessati e per il Garante per ogni questione attinente l'applicazione del Regolamento.

Scopri di più su: www.garanteprivacy.it/home/doveri

https://www.garanteprivacy.it/home/doveri

Entrata in vigore e operatività

Art. 99 RGDP: il nuovo regolamento si applica dal **25 maggio 2018** (ma è in vigore dal 25 maggio 2016)

Sistema delle fonti

- ✓ Regolamento 2016/679/UE
- ✓ d.lgs. 30 giugno 2003, n. 196 e s.m.i. (da ultimo modificato dal **d.lgs. 10 agosto 2018, n. 101, in vigore dal 19 settembre 2018**)
- ✓ Convenzione EDU, Carta diritti sociali fondamentali dell'UE, Raccomandazioni Cons. Europa, Convenzioni internazionali

A cosa serve il Regolamento UE?

Doppia ‘anima’ della disciplina:

a) tutela delle persone con riguardo al trattamento dei dati
b) diritto alla circolazione dei dati

si tratta di diritti non assoluti …
… nel senso che il diritto alla protezione dei dati (che è strumentale alla tutela delle persone) deve sopportare affievolimenti (rischi consentiti) e il diritto alla circolazione dei dati deve sopportare alcune condizioni, anche onerose
cfr. art. 1 …

A cosa serve il Regolamento UE?

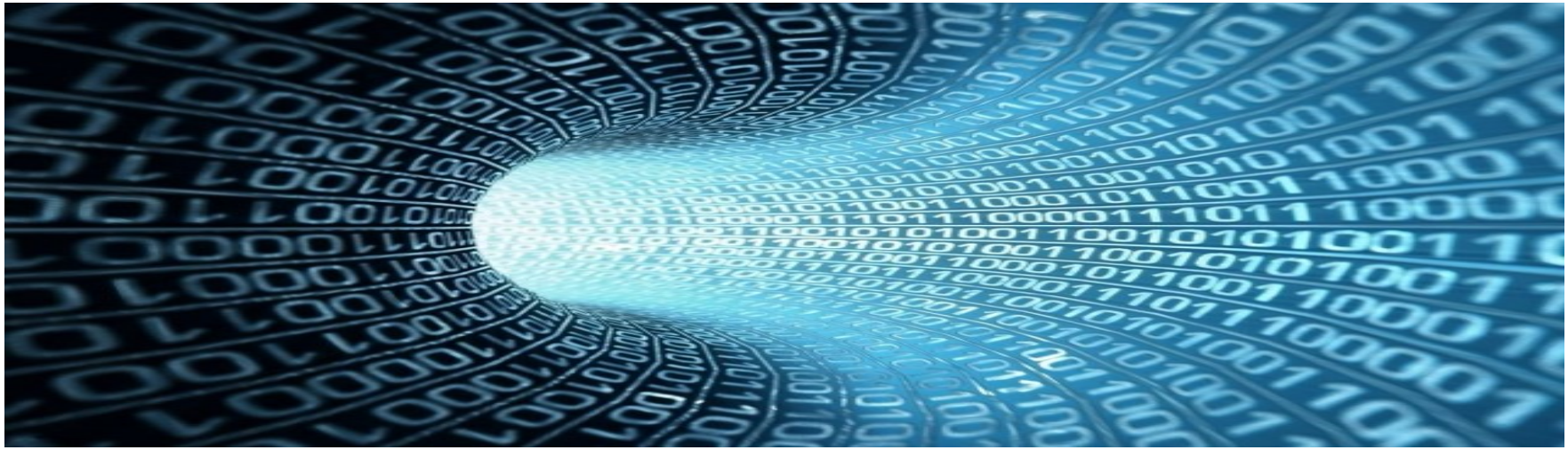
1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati

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

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

The processing of personal data should be designed to serve mankind

Nuovo paradigma?



Grande enfasi sul momento circolatorio dei dati personali (liceità, trasparenza, obblighi in capo al titolare e al responsabile, tenuta registri delle attività svolte, misure di sicurezza, notifica e comunicazione della violazione dei dati personali, valutazione d'impatto, codici di condotta).
Big data analytics: attenzione non tanto sul singolo individuo ma sui comportamenti di interi gruppi di individui, privi di una specifica connotazione sociale ma aggregati sulla base dei fini specifici del trattamento grazie a complessi algoritmi

Nuovo paradigma?

Il rispetto della privacy è una condizione necessaria per flussi commerciali stabili, sicuri e competitivi a livello mondiale. La privacy non è una merce di scambio. Internet e la digitalizzazione dei beni e dei servizi ha trasformato l'economia globale: il trasferimento transfrontaliero di dati, compresi i dati personali, è parte dell'operatività quotidiana delle imprese europee di tutte le dimensioni e in tutti i settori. Poiché gli scambi commerciali utilizzano sempre più i flussi di dati personali, la riservatezza e la sicurezza di tali dati è diventata un fattore essenziale della fiducia dei consumatori

(Comunicazione della Commissione COM(2017)7 final – Bruxelles 10 gennaio 2017 – scambio e protezione dei dati personali in un mondo globalizzato)

Nuovo paradigma

Approccio ‘ex ante’

Considerando 84 Reg. 2016/679 UE: valutazione d’impatto … esito della valutazione da prendere in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento

La valutazione d'impatto

Art. 35, co. 7, lett. a) Reg. 2016/679: la valutazione (d'impatto) contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento

b) valutazione della necessità e proporzionalità

c) valutazione dei rischi

La novità più importante

Responsabilizzazione («accountability»)

Il Regolamento tende a non definire adempimenti specifici, ma a definire principi di conformità.
Il titolare deve implementare i propri processi per raggiungere tali obiettivi. In assenza di specifici adempimenti viene valutata l'impostazione complessiva dei trattamenti riguardo ai rischi che ne derivano. Il titolare dunque sarà valutato a posteriori, in un'eventuale verifica, sull'adeguatezza dei propri comportamenti. Questo principio è applicato innanzitutto nella gestione della sicurezza e protezione dei dati personali

Approccio globale al sistema privacy

L’ambito di applicazione territoriale

Il Regolamento si applica:

1) ai trattamenti effettuati da titolari stabiliti nell’UE, indipendentemente dal fatto che il trattamento sia effettuato o meno nella UE
2) ai trattamenti effettuati da titolari non stabiliti nell’UE se il trattamento ha ad oggetto dati personali di interessati che si trovino nell’Unione e riguarda a) l’offerta di beni e servizi (anche non a pagamento) ai suddetti interessati, b) il monitoraggio di comportamenti che abbiano luogo nel territorio dell’UE

L’ambito di applicazione materiale

Il Regolamento si applica solo al trattamento dei dati personali di persone fisiche

Il Regolamento si applica a trattamenti interamente o parzialmente automatizzati e ai trattamenti non automatizzati, se i dati personali sono contenuti in un archivio o sono destinati a confluirvi

Il Regolamento non si applica ai trattamenti di dati personali effettuati:

- ✓ **da una persona fisica per l’esercizio di attività a carattere esclusivamente personale o domestico**
- ✓ **da un’autorità di pubblica sicurezza**
- ✓ **per attività che non rientrano nell’ambito di applicazione del diritto dell’UE**

I dati personali nel Regolamento

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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

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 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

I dati personali nel Regolamento

Art. 10 Reg.: trattamento dei 'dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza'.

Permangono definizioni ad hoc di:

- ✓ **dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione**
- ✓ **dati biometrici: 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 faciale o i dati dattiloscopici**

I dati personali nel Regolamento

Non esiste più una specifica definizione di dati personali 'sensibili' o di dati personali 'giudiziari', ma il concetto è comunque ricavabile

L'art. 9 individua in generale le "categorie particolari di dati personali": si tratta delle informazioni "che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica"

Nuova definizione di "dati relativi alla salute": "dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute"

I dati personali nel Regolamento

Nuove definizioni:

- ✓ **pseudonimizzazione: trattamento volto a nascondere l'identità dell'interessato e a impedirne l'identificazione senza l'utilizzo di informazioni aggiuntive. A tal fine le informazioni aggiuntive devono essere conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile**
- ✓ **profilazione: trattamento automatizzato finalizzato alla valutazione di determinati aspetti di una persona fisica come il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti. In linea generale la profilazione è vietata. È ammessa in circostanze specifiche e previo consenso dell'interessato. I trattamenti di profilazione rappresentano uno dei presupposti che rendono obbligatoria la valutazione preventiva di impatto sulla protezione dei dati**

I principi generali

- ✓ **Liceità**
- ✓ **Correttezza**
- ✓ **Trasparenza**
- ✓ **Limitazione delle finalità**
- ✓ **Minimizzazione dei dati**
- ✓ **Esattezza**
- ✓ **Limitazione della conservazione**
- ✓ **Integrità e riservatezza**

Nota Bene

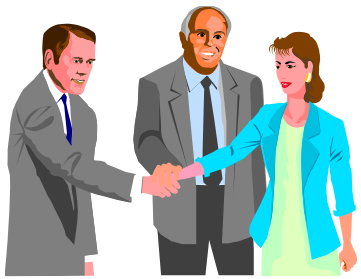
Responsabilizzazione del titolare del trattamento: ha l'obbligo di osservare il Regolamento e deve essere 'in grado di comprovarlo'

I soggetti della filiera privacy

PER RISPETTARE I VARI PASSAGGI IMPOSTI DALLA NORMATIVA OCCORRE DOTARSI DI UNA

STRUTTURA ORGANIZZATIVA ADATTA

A RISPONDERE CON FLESSIBILITA' ALLE RICHIESTE DI OGNI INTERESSATO IN RELAZIONE AL TRATTAMENTO SPECIFICO DEI DATI CHE LO RIGUARDANO



I soggetti della filiera privacy

Le figure soggettive privacy tipiche restano sostanzialmente invariate:

- ✓ **Titolare: 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**
- ✓ **Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento**
- ✓ **Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le *persone autorizzate al trattamento* dei dati personali sotto l'autorità diretta del titolare o del responsabile**

I soggetti della filiera privacy

Nuovo art. 2-quaterdecies del Codice privacy

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

Il titolare e 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

Figura nuova: Responsabile della protezione dei dati/DPO (art. 37 - linee guida WP 243/2016)

…

Il DPO: quando?

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

- ✓ **Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali**
- ✓ **Le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala**
- ✓ **Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10**

In tutti gli altri casi la nomina è facoltativa

L’informativa

L’informativa

Nell’informativa il titolare deve inserire obbligatoriamente **anche**:

- i **dati di contatto** del nuovo DPO ove previsto
- la **base giuridica** del trattamento a corredo dell’illustrazione delle finalità del trattamento
- qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare o di terzi, la **specificazione di quali siano i legittimi interessi** perseguiti dal titolare o da terzi
- l’**ambito del trasferimento all’estero** o ad un’organizzazione internazionale dei dati personali
- il **periodo di conservazione** dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo
- la specifica esistenza del **diritto alla portabilità** dei dati
- l’esistenza del **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca
- il diritto di **proporre reclamo** al Garante privacy

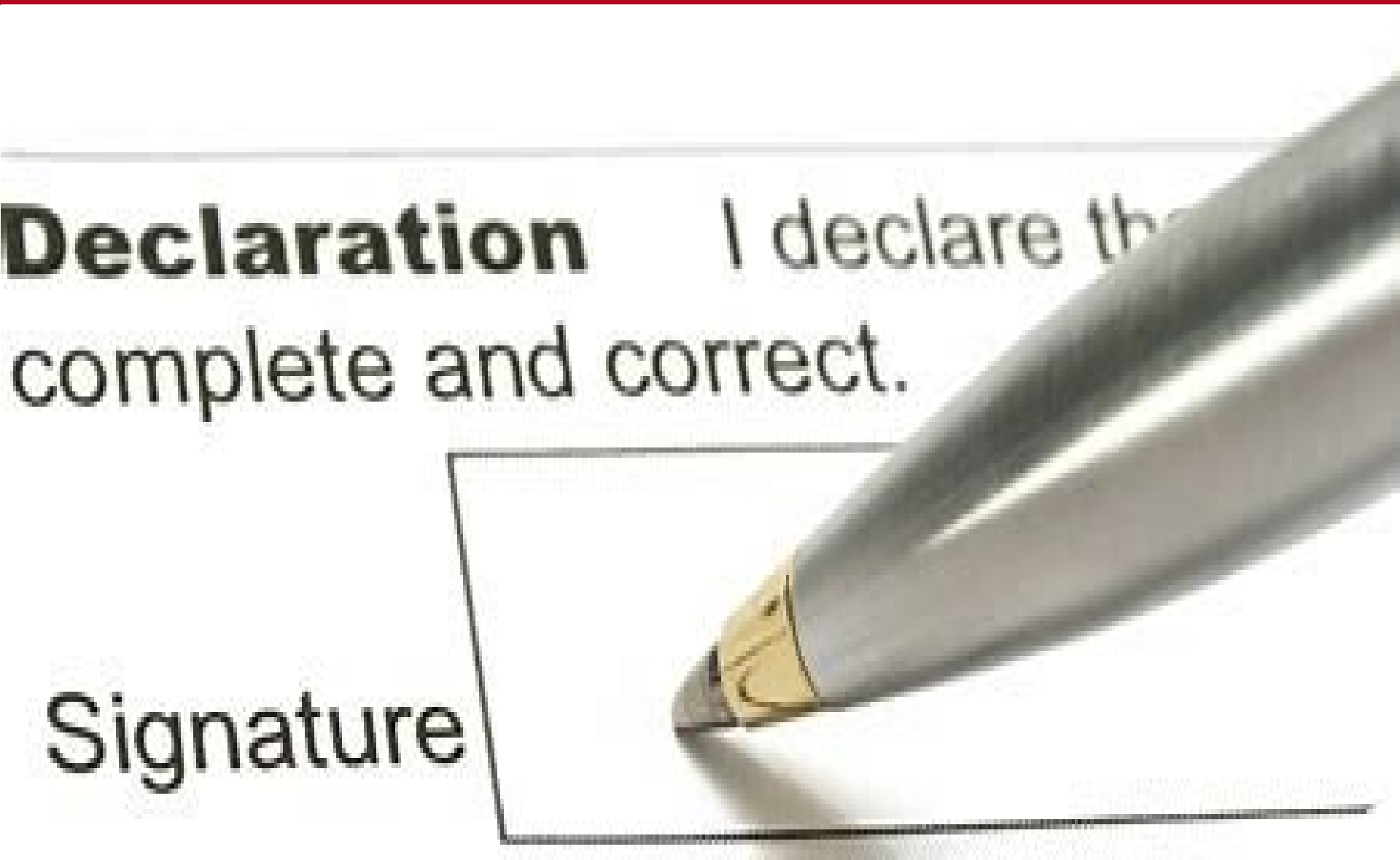
L’informativa

- l’eventuale esistenza di un **processo decisionale automatizzato**, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l’importanza e le conseguenze previste di tale trattamento per l’interessato
- la **fonte** da cui hanno origine i dati personali e, se del caso, l’eventualità che i dati provengano da fonti accessibili al pubblico (informazione questa obbligatoria solo ove i dati non siano raccolti presso l’interessato)
- le **categorie** di dati personali oggetto di trattamento (anche qui solo se i dati non siano raccolti presso l’interessato)

Le informazioni da rendere agli interessati possono essere fornite anche in combinazione con **icone standardizzate** per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un **quadro d’insieme del trattamento previsto**

Se presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo

Il consenso



Il Regolamento fonda sul ‘consenso dell’interessato’ la principale precondizione (salve le deroghe) di liceità del trattamento

(cfr. artt. 6 e 7)

Il consenso nel Regolamento

Consenso: qualsiasi manifestazione di volontà libera, specifica, informata e **inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva **inequivocabile**, che i dati personali che lo riguardano siano oggetto di trattamento

Il consenso nel Regolamento

L'interessato ha il **diritto di revocare il proprio consenso** (deve essere informato di questo diritto) in qualsiasi momento, con modalità di esecuzione della revoca del consenso facili come la sua prestazione originaria

La revoca non pregiudica la liceità del trattamento fino a quel momento effettuato

Attenzione all'art. 17 (c.d. diritto all'oblio): cancellazione dei dati se non sussiste altro fondamento giuridico per il trattamento

Il consenso nel Regolamento

L’esecuzione di un contratto o la prestazione di un servizio **non possono** essere condizionati alla prestazione del consenso al trattamento di dati personali **non necessario** all’esecuzione del contratto o servizio

Il consenso nel Regolamento

Alla **specifica manifestazione del consenso** è subordinata:

- la liceità del trattamento (altrimenti vietato salvo ricorrano i presupposti alternativi al consenso di cui all'art. 9 Reg.) dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dei dati genetici, biometrici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona
- la possibilità, altrimenti vietata, di procedere alla **profilazione** dell'interessato
- la possibilità di **trasferire i dati personali verso un paese terzo extra UE** o verso un'organizzazione internazionale

La **sicurezza nel trattamento dei dati è uno dei principi fondamentali del nuovo Regolamento europeo**. Si veda l'art. 5 che esprime il principio della integrità e riservatezza

La protezione dei dati personali

- ✓ **L'approccio alle misure di sicurezza e protezione dei dati personali è totalmente responsabilizzante nei confronti del titolare del trattamento**
- ✓ **Non esiste un corrispondente delle misure minime di sicurezza come erano definite nel disciplinare tecnico**
- ✓ **L'obbligo non è solo quello di adottare misure di sicurezza ma quello – più esteso e impegnativo – di definire politiche di sicurezza**
- ✓ **Tra gli obblighi di sicurezza vi è anche quello di essere in grado di dimostrare le politiche di sicurezza**

La gestione della sicurezza nel Regolamento

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:

- ✓ **La pseudonimizzazione e la cifratura dei dati personali**
- ✓ **La capacità di assicurare su base permanente la riservatezza, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento**
- ✓ **La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**
- ✓ **Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**

Organizzazione e gestione della sicurezza

Creare l'ambiente	Sensibilizzare il top management Sensibilizzare il personale Formare il personale Sensibilizzare e formare il personale ICT
Scegliere le tecnologie	Implementare le misure tecniche
Documentare	Definire le procedure operative
Controllare	Definire gli audit Svolgere gli audit Documentare i risultati degli audit
Agire	Relazionare il top management sugli esiti degli audit Valutare gli audit con il top management Pianificare i miglioramenti
Monitorare	Controllare gli incidenti Documentare gli incidenti

Le misure di sicurezza

Art. 32 Reg.: tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare e il responsabile devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza **adeguato al rischio**, che comprendano, tra le altre:

- la **pseudonomizzazione** e la **cifratura** dei dati personali
- la capacità di **assicurare** su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- la capacità di **ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- una procedura per **testare, verificare e valutare** regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Le misure di sicurezza

Quanto agli **obblighi di documentazione delle misure di sicurezza** (analoghi al vecchio DPS) il Regolamento prevede, ove possibile, di inserire nel nuovo **registro delle attività di trattamento** svolte una descrizione generale delle misure di sicurezza tecniche e organizzative

Inoltre, nella documentazione della valutazione preventiva di impatto sulla protezione dei dati, il titolare deve descrivere anche le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone

Privacy by design

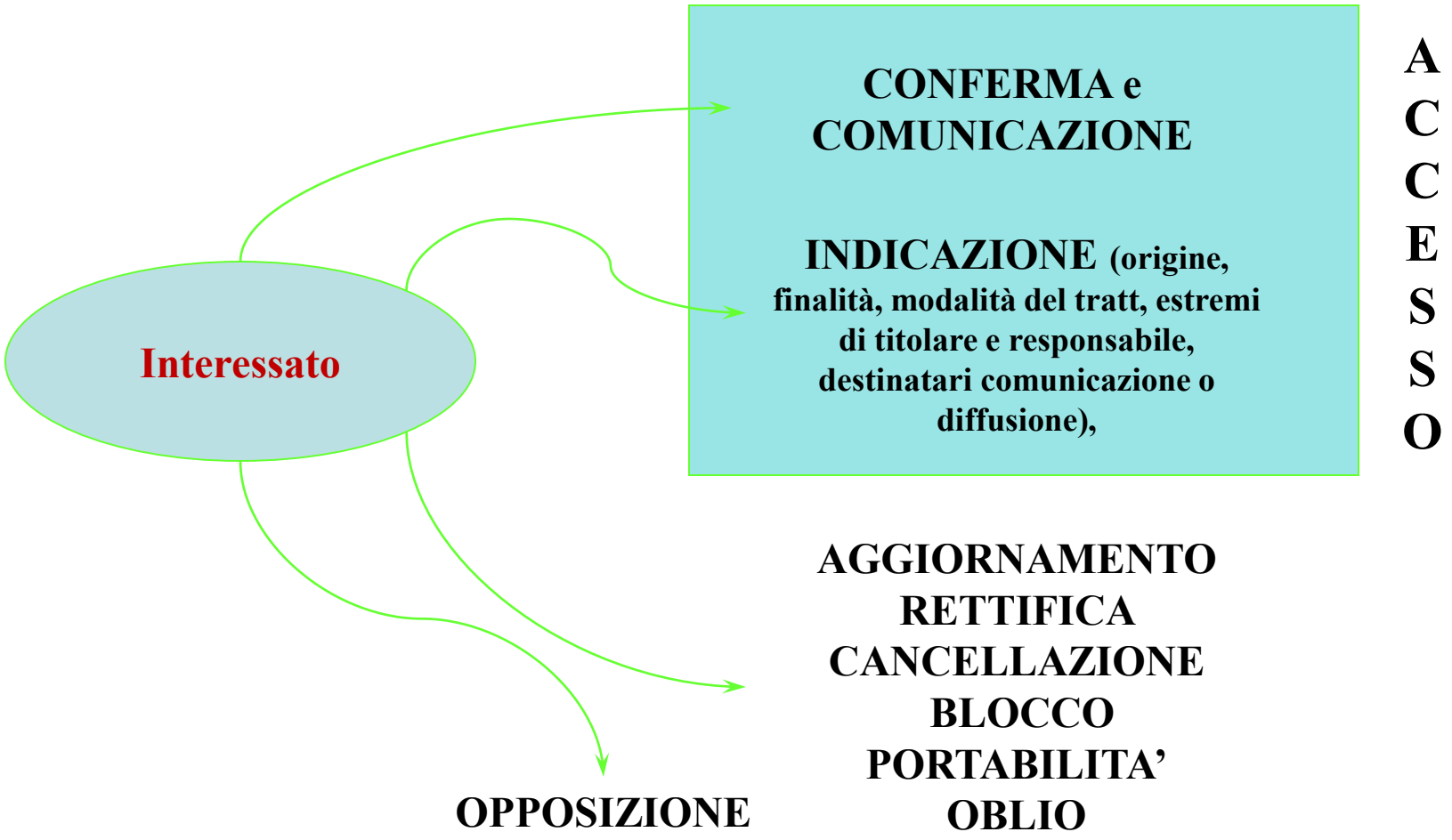
Privacy by design: il titolare del trattamento (tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento) deve applicare **misure tecniche e organizzative adeguate** (es. anonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie per tutelare i diritti degli interessati. Tale adempimento va effettuato sia al momento di determinare i mezzi del trattamento (es. progettazione di device) sia all'atto del trattamento stesso

Privacy by default

Privacy by default: il titolare deve mettere in atto misure tecniche e organizzative adeguate **per garantire che siano trattati, per impostazione predefinita** (by default) **solo i dati personali necessari per ogni specifica finalità del** trattamento

Il titolare può ottenere una **certificazione** *ad hoc*, prevista dal Regolamento in base ad una specifica procedura, per dimostrare la conformità ai principi di privacy by design e by default (artt. 42-43)

I diritti dell'interessato


CONFERMA e
COMUNICAZIONE
INDICAZIONE (origine, finalità, modalità del tratt, estremi di titolare e responsabile, destinatari comunicazione o diffusione),
ACCESSO
Interessato
AGGIORNAMENTO
RETTIFICA
CANCELLAZIONE
BLOCCO
PORTABILITA'
OBLIO
OPPOSIZIONE

Responsabilità e sanzioni

Responsabilità e sanzioni

Responsabilità civile: «chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento» (art. 82)

Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile

Responsabilità e sanzioni

Sanzioni amministrative pecuniarie

- ✓ fino a 10,000,000 di Euro per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazione di determinati obblighi imposti dal Regolamento (es. designazione responsabile del trattamento e DPO)
- ✓ fino a 20,000,000 di euro per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazione degli obblighi ritenuti più rilevanti (es. violazione principi generali art. 5)

Sanzioni penali

non è materia di competenza dell'UE. È compito degli Stati membri stabilire (e notificare alla Commissione entro il 25 maggio 2018) le norme relative alle altre sanzioni per le violazioni del Regolamento e adottare tutti i provvedimenti necessari per assicurare l'applicazione di sanzioni effettive, proporzionate e dissuasive