

Università degli Studi di Catania

La tutela della riservatezza  
e il trattamento dei dati personali  
nel GDPR

Seminario del corso di Digital forensics

Ignazio Zangara

Corso di laurea in Informatica

Anno accademico 2020/2021

PRIVACY

Principio passivo

Erigere un confine  
invalicabile, non  
oltrepassabile, a  
protezione del singolo e  
delle sue informazioni  
personali senza il suo  
consenso esplicito

Principio attivo

La libertà di poter  
compiere scelte  
personali ed intime in  
piena autonomia e  
senza il pericolo di  
essere condizionato,  
etichettato e influenzato

Convenzione Europea per la salvaguardia dei  
diritti dell'uomo e delle libertà fondamentali

Convenzione internazionale proclamata dall'Assemblea delle Nazioni Unite il 10 dicembre 1948 e firmata a Roma il 4 novembre 1950 dai Governi, membri del Consiglio d'Europa

Articolo 8 - Diritto al rispetto della vita privata e familiare

1. Ogni persona ha **diritto al rispetto** della sua **vita privata** (anche virtuale) e **familiare**, del suo **domicilio** (anche informatico) e della sua **corrispondenza** (anche elettronica)

2. Non può esservi ingerenza di una **autorità pubblica** nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la **sicurezza nazionale**, per la **pubblica sicurezza**, per il **benessere economico del paese**, per la **difesa dell'ordine** e per la **prevenzione dei reati**, per la **protezione della salute** o della **morale**, o per la **protezione dei diritti** e delle **libertà altrui**

Ogni individuo ha il diritto di richiedere la tutela dei diritti garantiti nella CEDU, attraverso il ricorso alla Corte europea dei diritti dell'uomo (Strasburgo) (*sussidiario*)

Disponibilità del diritto alla riservatezza

Il diritto alla riservatezza è un **diritto disponibile** e, quindi, **liberamente negoziabile**

La riservatezza è un **diritto assoluto** (può farsi valere *erga omnes*, anche nei confronti di coloro che ne hanno avuto la disponibilità), **ma rinunciabile** attraverso il **libero consenso** dell'interessato o di chi ne esercita la patria potestà

Il trattamento dei dati personali  
nell'ordinamento giuridico italiano

La prima legge italiana sulla protezione dei dati personali è la n. 675 del 31/12/1996, denominata *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*

**Il 1 gennaio 2004 entra in vigore il decreto legislativo n. 196 del 30/06/2003 - Codice in materia di protezione dei dati personali**

Il Codice - che rappresenta il primo tentativo al mondo di comporre in maniera organica le innumerevoli disposizioni relative, anche in via indiretta, alla tutela dei dati personali - riunisce in unico contesto la legge 675/1996 e gli altri provvedimenti normativi che si sono succeduti negli anni

Dal 25 maggio 2018 è pienamente applicabile il  
Regolamento generale sulla protezione dei dati  
Regolamento UE 2016/679 (GDPR)

Ha lo scopo di armonizzare la normativa in materia di protezione e di libera circolazione dei dati personali nei 27 Stati membri dell'Unione europea

D.Lgs. del 10 agosto 2018 n. 101 di adeguamento del nostro Codice al GDPR

Nozione contenuta nel GDPR

Riservatezza dei dati è oggi intesa come diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono un bene primario della società dell'informazione.



Figure chiave

- Garante – *Data protection supervisor*
- Titolare – *Data controller*
- Responsabile del trattamento – *Data processor*
- Responsabile della protezione dei dati – *Data protection officer*
- Incaricato →
  - persone autorizzate al trattamento
  - sotto l'autorità diretta del T o del R
  - (art. 4, punto 10)
- Interessato – *Data subject*

Titolare del trattamento

Il soggetto cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza

Titolare del trattamento (art. 24)

Tenuto conto della **natura**, dell'**ambito di applicazione**, del **contesto** e delle **finalità** del trattamento, nonché dei **rischi** aventi probabilità e gravità diverse per i **diritti** e le **libertà** delle persone fisiche, il T mette in atto **misure tecniche e organizzative adeguate** per garantire, ed essere in grado di dimostrare, che il **trattamento** è effettuato **conformemente** al Regolamento

Responsabile del trattamento

Il soggetto designato dal Titolare del trattamento, che tratta dati personali per conto di quest'ultimo



Novità introdotta dal Regolamento europeo

Principio dell'accountability (art. 24)  
Pilastro del GDPR che determina un cambio di prospettiva: non più adozione di misure minime per garantire il corretto trattamento dei dati personali, ma responsabilizzazione del T e del R che devono poter **rendicontare l'operato** dimostrando di aver adottato misure idonee e documentare, all'occorrenza, l'affidabilità e la competenza nella gestione dei dati personali

Novità introdotta dal Regolamento europeo

Data protection officer  
L'art. 37 afferma che tutti gli enti pubblici devono nominare un **Responsabile della protezione dei dati**. Il DPO è richiesto, inoltre, laddove le attività principali del T e del R di dati prevedano un monitoraggio regolare e sistematico su larga scala delle persone interessate, o qualora la società svolga attività di elaborazione su larga scala di categorie particolari di dati personali



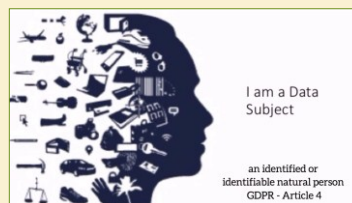
## Compiti ex art. 39

- **informare e fornire consulenza** al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR
- **sorvegliare** l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati
- fornire, se richiesto, un **parere** in merito alla **valutazione d'impatto sulla protezione** dei dati
- fungere da **punto di contatto** per il Garante per la protezione dei dati personali per questioni connesse al trattamento

**Da svolgere in piena autonomia e indipendenza**

## Interessato

La persona fisica cui si riferiscono i dati personali (identificata o identificabile tramite i dati personali oggetto del trattamento)



## 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**»

(art. 4, par. 1, GDPR)

## Categorie particolari di dati personali

«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»

Il divieto non si applica in presenza di consenso esplicito per finalità specifiche o di necessità per assolvere obblighi solo in determinati casi (art. 9, GDPR)

## Dati personali relativi a condanne penali e reati

«Il trattamento dei dati personali relativi alle **condanne penali** e ai **reati** o a **connesse misure di sicurezza** sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'Autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica»

(art. 10, GDPR)

## 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**

Liceità, minimizzazione, esattezza, trasparenza

Garanzie

Privacy by design

Il Regolamento intende richiamare l'attenzione dei T sull'esigenza che la protezione dei dati personali venga garantita «fin dalla progettazione»

A questo proposito, l'art. 25 stabilisce che il T del trattamento dei dati personali deve **adottare** delle **misure tecniche e organizzative idonee** a dare concreta attuazione a quelle che sono le disposizioni e i principi in materia di protezione dei dati e garantire in questo modo i diritti degli interessati. La predisposizione delle misure necessarie è prescritta **sia** nel momento in cui il Titolare del trattamento debba **determinare i mezzi del trattamento** stesso, **sia** quando ponga in essere le vere e proprie **operazioni** di trattamento


Privacy by default

La protezione dei dati personali sia garantita per «impostazione predefinita»

Il trattamento di dati personali è lecito quando ...

L'Interessato ha espresso il proprio **consenso** per una o più specifiche finalità;  
È necessario per l'**esecuzione di un contratto** di cui l'Interessato è parte;  
È necessario per **adempiere ad un obbligo legale** al quale è soggetto il Titolare del trattamento;  
È necessario per **salvaguardare degli interessi vitali** dell'Interessato o di altre persone fisiche;  
È necessario per l'**esecuzione di un compito di pubblico interesse** o connesso all'**esercizio di pubblici poteri** di cui è investito il Titolare del trattamento;  
I dati personali sono conservati in una forma che consenta l'**identificazione** dell'Interessato per un **periodo di tempo non superiore a quello necessario** agli scopi per cui sono stati legittimamente raccolti e trattati.

Informativa (artt. 12-14)

L'informativa deve essere, di solito, fornita direttamente agli interessati al momento della raccolta dei dati. Deve prevedere **gesti positivi** dell'Interessato per la raccolta  del **consenso**.

Il contenuto è, **ad esempio**:

- l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante e del Responsabile
- finalità, strumenti e base giuridica del trattamento
- la natura obbligatoria o facoltativa del trattamento
- le eventuali conseguenze in caso di rifiuto nel comunicare i dati da parte dell'Interessato
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali
- i diritti dell'Interessato
- i dati di contatto del DPO (ove applicabile)
- periodo di conservazione dei dati (o i criteri per determinarlo)
- nuovi diritti degli Interessati: diritto alla portabilità dei dati; diritto di proporre reclamo ad un'Autorità di controllo


L'espressione del **consenso** al trattamento dei dati deve prevedere un'**azione positiva** da parte dell'Interessato

Acconsento



Non acconsento



Non è consentito prevedere modelli di raccolta del consenso precompilati  
La sottoscrizione per la manifestazione del consenso è preferibile 

ESEMPIO DI RACCOLTA DEL CONSENSO AI TRATTAMENTI DEI DATI PERSONALI (granularità)

Preso atto dell'Informativa

Acconsento al trattamento dei dati personali finalizzato all'acquisto dei beni e dei servizi forniti tramite questo sito web e riservati agli utenti registrati, che la Società X utilizzerà, anche per l'eventuale esecuzione degli obblighi contrattuali inerenti l'acquisto dei beni e la fruizione dei servizi da essa proposti. L'eventuale diniego non consentirà alla Società X di perfezionare la registrazione dell'utente sul proprio sito web né di accettare la proposta di acquisto dei prodotti o dei servizi offerti.

☒ Accanto\* ☐ Non Accanto

Acconsento al trattamento dei dati personali, anche con modalità automatizzate, finalizzato all'invio di comunicazioni relative a prodotti e servizi della Società X, al fine di ricevere materiale informativo, promozionale e/o partecipare a ricerche di mercato mediante diversi mezzi di comunicazione. L'eventuale diniego non consentirà alla Società X di comunicare agli utenti sconti, promozioni, offerte, inviti e altre iniziative riservate agli utenti registrati.

☒ Accanto ☐ Non Accanto

Acconsento al trattamento dei dati personali, anche mediante modalità automatizzate, per personalizzare i servizi forniti e meglio indirizzare le proposte promozionali grazie ad attività di profilazione. L'eventuale diniego non consentirà alla Società X di effettuare comunicazioni personalizzate e selezionate relative a sconti, promozioni, offerte, inviti e altre iniziative dedicate agli utenti registrati.

☒ Accanto ☐ Non Accanto

Acconsento al trattamento dei dati personali, anche con modalità automatizzate, finalizzato all'invio di comunicazioni relative a prodotti e servizi di società terze, al fine di ricevere materiale informativo, promozionale e/o partecipare a ricerche di mercato mediante diversi mezzi di comunicazione. L'eventuale diniego non consentirà alla Società X di comunicare agli utenti sconti, promozioni, offerte, inviti e altre iniziative riservate agli utenti registrati.

☒ Accanto ☐ Non Accanto

Acconsento alla comunicazione e alla cessione a terze parti dei dati personali, anche con modalità automatizzate, per l'invio di comunicazioni di carattere commerciale su prodotti e servizi, nonché per l'invio di ricerche di mercato.

☒ Accanto ☐ Non Accanto

I campi contrassegnati con l'asterisco (\*) sono obbligatori. Il relativo diniego non consentirà alla Società X di perfezionare la registrazione dell'utente sul proprio sito web né di accettare la proposta di acquisto dei prodotti o dei servizi offerti.

Diritti dell'Interessato

I soggetti cui si riferiscono i dati personali, nella loro qualità di Interessati, hanno il diritto in qualunque momento di chiedere al Titolare del trattamento informazioni in merito all'esercizio dei propri diritti.

In sintesi, gli Interessati hanno diritto di:

- conoscere i contatti del Titolare e, ove previsto, del Responsabile del Trattamento nonché del Responsabile per la protezione dei dati
- ottenere la conferma dell'esistenza o meno dei propri dati e di conoscerne il contenuto e l'origine e le finalità
- chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi, la limitazione del trattamento che li riguardano, di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati
- revocare il consenso in qualsiasi momento, senza tuttavia pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca.
- proporre reclamo ad un'Autorità di controllo

**Diritto all’oblio (art. 17)**

L’interessato ha il diritto di ottenere dal titolare del



cancellazione altri Titolari che trattano i dati personali oggetto della richiesta di cancellazione, compresi ‘qualsiasi link, copia o riproduzione’

**Diritto alla portabilità dei dati (art. 20)**

L’**Interessato** ha il diritto di ricevere in un **formato strutturato, di uso comune e leggibile da dispositivo automatico** i dati personali che lo riguardano forniti ad un Titolare del trattamento e ha il diritto di **trasmettere tali dati a un altro Titolare** del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti 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.

L’interessato ha, inoltre, il diritto di ottenere la **trasmissione diretta** dei dati da un Titolare del trattamento all’altro, *se tecnicamente fattibile*.



**La valutazione d’impatto sulla protezione dei dati**  
Data Protection Impact Assessment – DPIA (artt. 35-36)

Quando **un tipo di trattamento**, allorché preveda 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

È un **processo** che aiuta a **gestire i rischi** connessi al trattamento dei dati personali per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali mediante l’analisi del trattamento e la valutazione dei principi di **proporzionalità e necessità** ad esso correlati, identificando i rischi connessi e contribuendo a individuare le misure e accorgimenti necessari per mitigare tali rischi

**Data breach**



Il Regolamento prevede espressamente l’**obbligo del Titolare di notificare la violazione al Garante per la protezione dei dati personali, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche**

L’art. 33 impone al titolare di notificare la violazione all’Autorità di controllo, ove possibile, **entro 72 ore** dal momento in cui ne viene a conoscenza. Il tempo di riferimento da cui iniziano a decorrere i termini della notifica viene individuato quindi nel momento in cui il Titolare acquisisce **consapevolezza** dell’avvenuta violazione

**Regime sanzionatorio (art. 83)**

La violazione delle norme poste a tutela della protezione dei dati resta soggetta all’applicazione delle **sanzioni amministrative pecuniarie**.

La definizione delle altre sanzioni (tra cui anche quelle penali) resta di competenza dei legislatori nazionali

I Responsabili del trattamento sono responsabili **in solido** per il risarcimento del danno con Titolari, Contitolari e altri Responsabili