Prof. Claudio Pantanali, PhD - cpantanali@units.it

GDPR
Privacy e tutela dei dati personali

20 March 2018

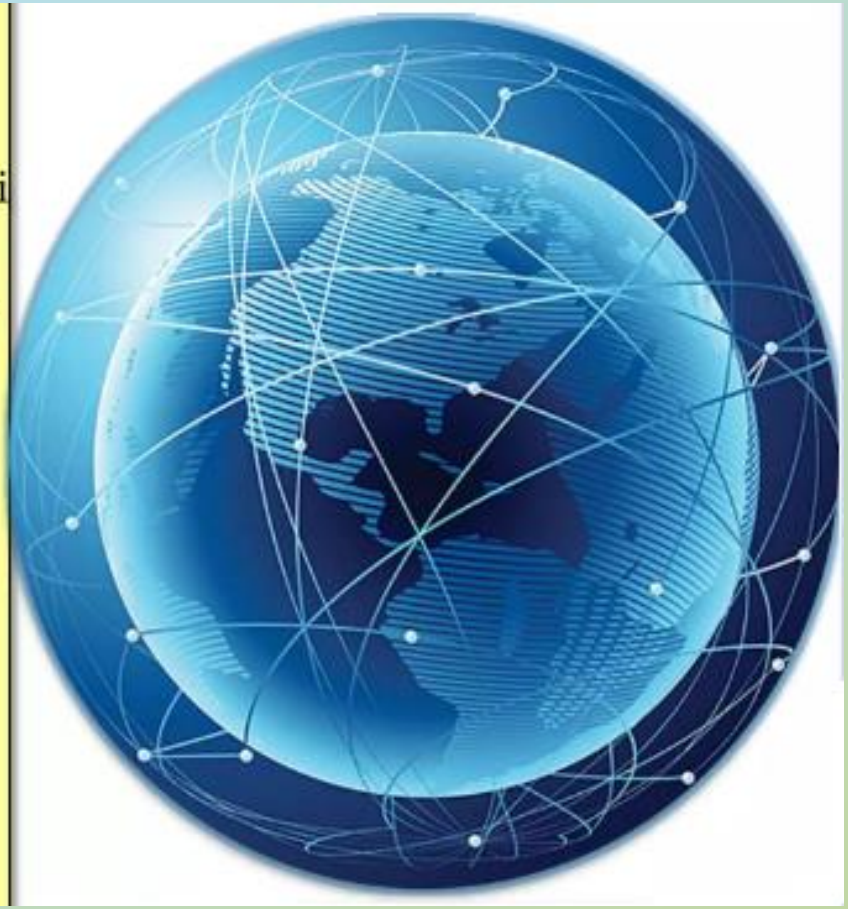
Prof. Claudio Pantanali, PhD - cpantanali@units.it

Perché il Mondo è cambiato

Il nuovo scenario digitale mostra che la Rete è pervasiva, immateriale e immediatamente disponibile a molti utenti

La rapidità e l'intensità
dell'evoluzione tecnologica
hanno condotto all'aumento di soggetti
ed oggetti connessi fra loro
(per questo si parla di rete delle cose,
Internet Of Things, IoT).

Si assiste al conseguente
scambio e condivisione di dati fra
Individui ed Organizzazioni
di diverso genere e tipo
(o scopo, quali Istituzioni, Imprese,
Enti no Profit, etc.)
in tutto il mondo
sia fisico che digitale.



Prof. Claudio Pantanali, PhD - cpantanali@units.it

Perché il Mondo è cambiato

Evoluzione della Tecnologia

Evoluzione e Sviluppo dell'Economia Digitale

Difficoltà a garantire efficacemente la protezione dei dati personali dei cittadini

Necessità di regole uniformi in tutti i Paesi EU

Diritto alla Privacy
(limite alla libertà di informazione)

→ **Diritto alla protezione dei dati personali**
(difesa dal controllo sulle persone)

DATI PERSONALI → LIBERTÀ E DIRITTI

Prof. Claudio Pantanali, PhD - cpantanali@units.it

CHE COS'E' IL GENERAL DATA PROTECTION REGULATION?

- Dopo **4 anni** di preparazione e dibattito è stato approvato il **GDPR** dal Parlamento Europeo il **27 aprile 2016**.
- Come prevede l'art. 99 il Regolamento si applicherà **a decorrere dal 25 maggio 2018**
- Il nuovo Regolamento Generale Europeo sulla Protezione dei Dati Personali n. 2016/679 (GDPR), con i suoi 99 articoli ha **riscritto la disciplina della Privacy a livello europeo.**
- La necessità di emanare un Regolamento Europeo in materia di privacy nasce dalla **continua evoluzione** degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente **alla diffusione del progresso tecnologico.**
- Quando si parla di privacy parliamo di dati relativi alle Persone Fisiche

Prof. Claudio Pantanali, PhD - cpantanali@units.it

La protezione dei dati personali è un diritto fondamentale
(art. 8 par. 1 Carta dei diritti fondamentali dell'Unione Europea)

Il diritto alla protezione dei dati non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e contemperato con altri diritti fondamentali

Al fine di assicurare un livello coerente e elevato di protezione delle persone e rimuovere gli ostacoli alla circolazione dei dati personali, il livello di protezione dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali deve essere equivalente in tutti gli Stati membri

Prof. Claudio Pantanali, PhD - cpantanali@units.it

- **General Data Protection Regulation** (GDPR) è il Regolamento Europeo 2016/679 che riguarda la **Protezione dei dati personali delle Persone fisiche**

- **Aggiorna e abroga la "Direttiva Madre" (95/46/CE),** ormai superata (recepita dall'attuale D.Lgs 196/2003, il c.d. Codice Privacy)

- È stato realizzato per **potenziare e unire i diritti sulla Privacy online e la Protezione dei dati personali all'interno dell'Unione Europea** (EU) e al tempo stesso velocizzare gli obblighi delle imprese al servizio dei cittadini EU

- **Amplia il concetto di dato personale** - qualunque tipo di informazione riferita/riferibile a persona **indipendentemente dal contesto** (privato/vita familiare o altra attività); **dalla forma** (caratteristiche, es. alfabetica, numerica, fotografica, acustica); **dal supporto** (carta, HD, video, ecc.)

- **Si applicherà in maniera ubiquitaria in tutti i 27 paesi EU**, mediante **un unico Regolamento al posto delle attuali leggi nazionali** a partire **dal 25 Maggio 2018**

Prof. Claudio Pantanali, PhD - cpantanali@units.it

- Il GDPR quindi non è la 'nuova legge sulla privacy', ossia non abroga in toto il vecchio D.lgs 196/2003 ma **ne rivede le finalità** estendendo, tra le altre cose, il concetto di '**protezione dei dati personali**'.
- Il GDPR è una legge che **riguarda tutte le aziende che lavorano in Europa**, ovunque siano site, sia pubbliche che private, indipendentemente dalla dimensione.
- Il GDPR **non potrà subire** '**deroghe**' poiché non dovrà essere recepito dalla nostra legislazione nazionale
- Il GDPR **si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali**

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Regolamento 2016/679	**IN VIGORE,** pienamente applicabile dal 25 maggio 2018
Direttiva 1995/46	**IN VIGORE,** decade il 24 maggio 2018
Codice D.Lgs. 196/2003	**VIGORE, NON DECADE**, dovrà essere coordinato con il reg. UE secondo i criteri indicati dalla Legge di Delegazione
Provvedimenti Autorità Garante	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati
Accordi Internazionali su Trasferimento dati	**VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissioni UE	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificate, sostituite, abrogate

Direttiva 95/46/CE sulla protezione dei dati personali.
Gli Stati membri garantiscono, conformemente alle disposizioni della direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

I principi fondamentali del GDPR

Alcuni concetti importanti (Art.4 del regolamento UE 2016/679)

- **Dato personale**: «qualsiasi i**nformazione 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».
- **Dato particolare** (Dato sensibile per il *Codice Privacy*): **informazioni particolari relative alle persone** e ad informazioni genetiche➔ biometriche➔ relative alla salute➔ a condanne penali ed ai reati o a connesse misure di sicurezza (non esiste una lista ma solo dei criteri).
- **Profilazione**: «**qualsiasi forma di trattamento automatizzato di dati personali** consistente **nell'utilizzo di tali dati personali per valutare** determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»;

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Principi da rispettare

- **Principio di liceità, correttezza e trasparenza**: il principio di liceità del trattamento dei dati personali stabilisce che i dati personali devono essere trattati lealmente e lecitamente, quindi nel rispetto delle leggi, anche di quelle che regolano settori specifici.
- **Principio di limitazione delle finalità**: i dati personali devono essere raccolti per finalità determinate,esplicite e legittime e successivamente trattati in modi non incompatibili con tali finalità iniziali (ad esclusione delle raccolte per interesse pubblico, scientifico, statistico o storico);
- **Principio di minimizzazione dei dati**: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **Principio dell'esattezza**: i dati personali devono essere 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.
- **Principio della limitazione della conservazione**: i dati personali sono 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 (fanno eccezione, come prima menzionato, quelli raccolti per interesse pubblico);
- **Principio dell'integrità e della riservatezza**: i dati personali sono 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;
- **Principio della responsabilizzazione**: Il titolare del trattamento è competente per il rispetto dei principi ora evidenziati e deve essere in grado di comprovarlo.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

I soggetti coinvolti nel trattamento dati

1) **INTERESSATO** (Data Subject): persona fisica a cui si riferiscono i dati
2) **TITOLARE DEL TRATTAMENTO** (Data Controller): decide mezzi e finalità del trattamento (solitamente è il legale rappresentante dell'azienda)
3) **RESPONSABILE DEL TRATTAMENTO** (Data Processor): tratta dati per conto del Data Controller (es. titolare dell'azienda fornitore del sistema gestionale in cloud)
4) **INCARICATO DEL TRATTAMENTO** (Authorised): persona fisica dipendente dalle figure n. 2 o 3 (Titolare/Responsabile)
5) **DESTINATARIO** (Recipient): chi riceve comunicazione di dati (es. titolare dell'azienda produttrice del software gestionale con cui si gestiranno i dati)
6) **DATA PROTECTION OFFICER (DPO):** non obbligatorio sotto i 250 dipendenti, si occupa di considerare i rischi inerenti al trattamento, «coadiuvare» il Titolare

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Diritti degli interessati:

- ACCESSO: Avere conferma che sia in corso un trattamento di dati e accesso agli stessi (copia)
- RETTIFICA: Ottenere la correzione o integrazione dei dati personali inesatti
- LIMITAZIONE DEL TRATTAMENTO: Richiedere la sola conservazione (illiceità del trattamento, mancata correttezza dei dati, particolare necessità dell'interessato)
- PORTABILITÀ: Ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico e richiederne trasmissione ad altro titolare del trattamento
- OBLIO: Decidere che siano cancellati tutti i dati personali non più necessari alle finalità
- OPPOSIZIONE: Opporsi in qualsiasi momento al trattamento automatizzato che abbia impatti significativi sulla sua libertà o diritti, compresa la profilazione
- RECLAMO: Reclamare all'Autorità Garante la Privacy per ogni presunta violazione del GDPR RICORSO GIURISDIZIONALE: Ricorrere in giudizio contro il Titolare ed eventuali responsabili del trattamento per violazioni al trattamento dei propri dati

Trasparenza del trattamento: L'informativa

- Deve essere **concisa, trasparente, intellegibile, semplice e chiara**.
- **Deve essere sempre resa** (anche non per iscritto) e **con mezzi comprovanti l'identità** dell'interessato.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Gli obblighi di Legge: **Il Data Breach**

Qualsiasi violazione dei dati personali deve essere documentata, quando il titolare ne viene a conoscenza (registro degli incidenti).

Se la violazione presenta rischi per i diritti e le libertà delle persone, il titolare è tenuto a notificarla alla Autorità di controllo entro 72 ore (il responsabile informa il titolare senza ritardo).

Se la violazione presenta alti rischi per i diritti e le libertà delle persone, il Titolare è tenuto ad informare anche gli interessati in modo chiaro, semplice e immediato e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Per essere documentata e poi notificata la violazione deve essere intercettata, dunque **deve essere progettata e implementata una serie di misure di prevenzione, monitoraggio, controllo su violazioni**.

La notifica deve descrivere la natura della violazione - Comunicare i riferimenti di un punto di contatto - Descrivere le probabili conseguenze della violazione - Descrivere le misure adottate o proposte per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

Il Titolare del trattamento **potrà decidere di non informare gli interessati**:

- se riterrà che la violazione non comporti un rischio elevato per i loro diritti
- dimostrerà di avere adottato misure di sicurezza a tutela dei dati violati (e.g. cifratura)
- sosterrà che informare gli interessati comporta uno sforzo sproporzionato, nel qual caso è richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile

L'Autorità di controllo potrà comunque imporre al Titolare del trattamento di informare gli interessati sulla base di una autonoma valutazione del rischio associato alla violazione.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

C'era una volta…

Con i faldoni era molto più semplice …
bastava un armadio con serratura!

Ma oggi:

Cloud Computing
Social Network,
Smartphone, tablet,
IoT, Big Data, Sentiment Analysis…

Come proteggersi ?

Regolamento europeo concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati

Regolamento europeo 2016/679

- ***approvato dal Parlamento europeo il 14 aprile 2016***
- ***in vigore dal 24 maggio 2016***
- ***direttamente applicabile dal 25 maggio 2018***

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Garante europeo della protezione dei dati (GEPD)

Il GEPD e i cittadini

Gli organi e le istituzioni dell'UE non devono trattare i dati personali riguardanti:

- **l'origine etnica o razziale**
- **le opinioni politiche**
- **le concezioni filosofiche o religiose**
- **l'affiliazione sindacale.**

Né possono trattare dati concernenti la **salute** o l'**orientamento sessuale** se non per scopi sanitari. Anche in questo caso, il trattamento deve essere eseguito da un professionista del settore sanitario o da altre persone tenute al segreto professionale.

Ove si ritenga che il proprio **diritto alla privacy sia stato violato** da un'istituzione o da un organo dell'UE, ci si dovrebbe **rivolgere** in prima istanza **al personale dell'UE responsabile del trattamento dei propri dati nel servizio in cui si ritiene sia stata commessa la violazione**. Se i risultati non sono soddisfacenti, contattare il responsabile della protezione dati dell'istituzione o dell'organo dell'UE che si ritiene abbia commesso la violazione.

Se ciò non ha effetto, si può **presentare un reclamo** al GEPD utilizzando un modulo apposito. Il Garante europeo della protezione dei dati **indagherà** e comunicherà agli interessati se concorda con il reclamo presentato e, in caso affermativo, come si sta procedendo a correggere la situazione.
Se **si è in disaccordo** con la decisione del GEPD, è possibile deferire la questione alla Corte di giustizia dell'UE.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

La tua Europa – Consulenza / SOLVIT

La tua Europa - Consulenza

La tua Europa - Consulenza è un **servizio di consulenza destinato al pubblico**, attualmente fornito dai giuristi dello European Citizen Action Service (ECAS), un'organizzazione esterna che opera per conto della Commissione europea. È costituito da un **gruppo di 65 giuristi indipendenti** che lavorano in **tutte le lingue ufficiali dell'UE** e conoscono sia la normativa europea che quella nazionale di tutti gli Stati membri. Hanno il compito di:

- fornire consulenze gratuite e personalizzate nella lingua prescelta **entro una settimana**
- **chiarire la normativa europea** applicabile a ogni caso
- spiegare ai cittadini dell'UE come esercitare i loro diritti.

Il servizio La tua Europa - Consulenza è operativo da oltre 25 anni e dal 1996 ha fornito consulenze personalizzate in più di 360 000 casi.

La tua Europa - Consulenza opera in stretta collaborazione con SOLVIT, una rete creata per risolvere i problemi incontrati da **cittadini o imprese** con le **amministrazioni di un altro paese** in casi di presunta errata applicazione del diritto dell'UE.

Se, dopo aver esaminato la richiesta di consulenza, riteniamo che potresti aver bisogno di un ulteriore aiuto per risolvere il problema con l'amministrazione nazionale in questione, provvederemo a trasferire il tuo caso a SOLVIT e ti informeremo di conseguenza.

Il servizio La tua Europa - Consulenza risponde a domande inviate da:

- **cittadini** dell'Unione europea, dell'Islanda, del Liechtenstein o della Norvegia
- **cittadini extra UE**, se sono familiari di un cittadino dell'UE o di una persona residente nell'UE
- **imprese** con sede nell'UE
- **servizi europei/nazionali di informazione e consulenza**, per conto di privati.

Domande riguardanti...

una **situazione reale** (non ipotetica), anche se si tratta della semplice intenzione di trasferirsi in un altro paese dell'UE
i tuoi diritti in **uno o più paesi dell'UE** ai sensi della normativa europea.

SOLVIT è un servizio **gratuito** fornito dall'**amministrazione nazionale** di ogni paese dell'UE e di Islanda, Liechtenstein e Norvegia. Si tratta **in prevalenza di un servizio online**. Sebbene in ogni paese esista un centro .

Per ogni caso segnalato, SOLVIT punta a trovare una soluzione entro **10 settimane** dal giorno in cui è stato notificato al centro SOLVIT del paese in cui il problema si è verificato.

Quando SOLVIT può essere d'aiuto

SOLVIT può intervenire:

- in caso di violazione dei diritti UE dei cittadini o delle imprese da parte della pubblica amministrazione di un altro paese dell'UE
- se non è stato avviato un procedimento giudiziario (può invece farlo nel caso di un semplice ricorso amministrativo).

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Il nuovo Regolamento europeo coordinamento normativo

Ove il regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone integrare elementi del regolamento nel proprio diritto nazionale

Per quanto riguarda il trattamento dei dati personali … per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del regolamento

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Il Regolamento detta la DISCIPLINA GENERALE

Normative nazionali per disciplina speciale e di settore

- ***Non abroga il D.Lgs. n. 196 del 2003***
- ***Disapplicazione di norme nazionali in contrasto con il regolamento***
- ***Applicazione di norme nazionali derogatorie (ove ammesso), integrative, speciali***

CAPI

- ***Disposizioni generali***
- ***Principi***
- ***Diritti dell'interessato***
- ***Titolare del trattamento e responsabile del trattamento***
- ***Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali***
- ***Autorità di controllo indipendenti***
- ***Cooperazione e coerenza***
- ***Mezzi di ricorso, responsabilità e sanzioni***
- ***Disposizioni relative a specifiche situazioni di trattamento***
- ***Atti delegati e atti di esecuzione***
- ***Disposizioni finali***

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Il nuovo Regolamento europeo ambito di applicazione materiale

SI APPLICA ai trattamenti:

- ***effettuati da un Titolare o Responsabile stabilito nell'UE, anche se il trattamento è effettuato fuori dall'UE***
- ***effettuati da un Titolare o Responsabile non stabilito nell'UE se il trattamento ha ad oggetto dati personali di interessati che si trovano nell'UE***
- ***effettuati da un Titolare stabilito in uno Stato extra UE soggetto al diritto di uno Stato UE in virtù del diritto internazionale***
- ***Si applica solo al trattamento di dati personali di persone fisiche***
- ***Riguarda trattamenti interamente o parzialmente automatizzati o non automatizzati se i dati personali sono contenuti in un archivio o sono destinati a confluirvi***

NON SI APPLICA ai trattamenti:

- ***effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico***
- ***di informazioni anonime o dati personali anonimizzati***
- ***per attività che non rientrano nel diritto dell'Unione (es. sicurezza nazionale)***
- ***per attività di speciale rilevanza pubblica (es. politica estera e di difesa comune)***
- ***effettuati da autorità ai fini di prevenzione, accertamento e repressione reati e ai fini di sicurezza pubblica***

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Art. 4 – definizioni: 196/2003 vs GDPR

196/2003	GDPR
"**dato personale**", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale	«**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

196/2003	GDPR
"**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;	«**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;

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Art. 4 – definizioni: 196/2003 vs GDPR

196/2003	GDPR
"**misure minime**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31	Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). **Principio di Accountability**

196/2003	GDPR
	«**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

196/2003	GDPR
Art. 33. Misure minime 1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.	Protezione dei dati fin dalla progettazione (by design) e protezione per impostazione predefinita (by default) …il titolare del trattamento mette in atto misure tecniche e organizzative adeguate… …per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento… (Principio di minimizzazione)

Prof. Claudio Pantanali, PhD - cpantanali@units.it

IMPIANTO SANZIONATORIO

Le violazioni agli obblighi in capo alle imprese (20 articoli su 49) sono punite **fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo**.

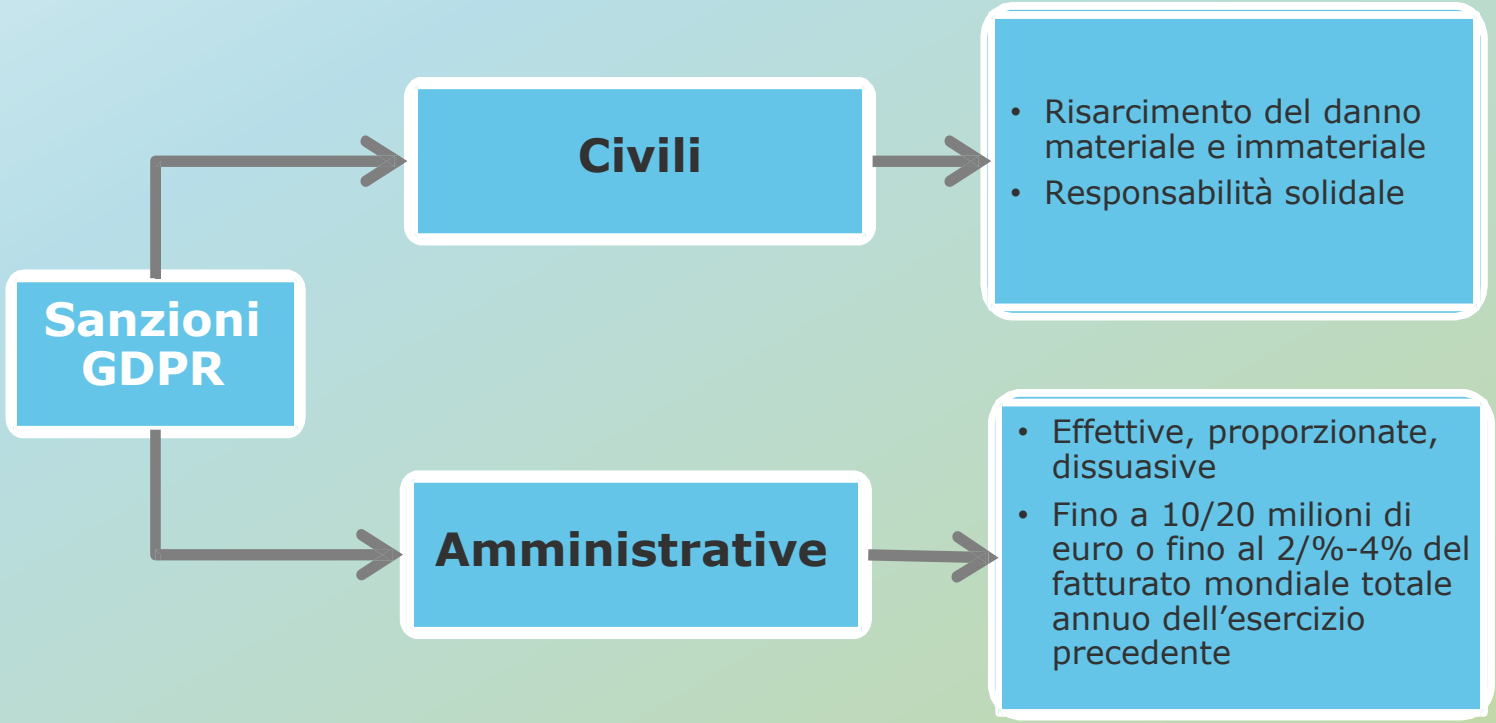
Ad esempio:

- la violazione dell'obbligo di tenuta del registro dei trattamenti;
- la mancata valutazione d'impatto DPIA;
- l'omessa consultazione preventiva dell'Autorità;
- l'omessa notifica di data breach;
- l'omessa nomina del DPO;
- l'omessa adozione di misure di sicurezza adeguate.

Gli altri 29 articoli puniscono **fino a 20 milioni di euro o fino al 4 % del fatturato mondiale annuo** la violazione dei principi del regolamento e dei diritti degli interessati.

Ad esempio:

- i principi di base del trattamento, comprese le condizioni relative al consenso;
- i diritti degli interessati;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.



Prof. Claudio Pantanali, PhD - cpantanali@units.it

NUOVI DIRITTI INDIVIDUALI

Diritto alla cancellazione (diritto all'oblio)

inteso come il diritto dell'interessato di ottenere dal titolare la cancellazione dei dati personali che lo riguardano in presenza di particolari condizioni

Diritto di limitazione di trattamento,

con cui l'interessato può chiedere una restrizione del trattamento

(ad es. la sola conservazione dei dati con esclusione di qualsiasi altro utilizzo)

CONSENSO

SPECIFICO E INFORMATO

Un consenso per ogni finalità

Preceduto dall'informativa

DIMOSTRABILE

Il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali (onere della prova)

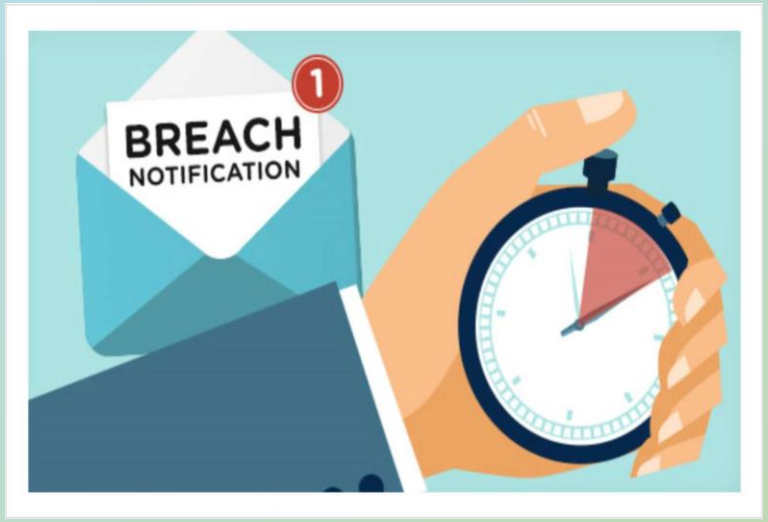
FACILITÀ DI REVOCA

ESPLICITO

Solo per il trattamento dei dati particolari e per la profilazione

All'interno di un contratto scritto la richiesta di consenso deve essere presentata in modo chiaramente distinguibile e con un linguaggio semplice e chiaro.

OBBLIGO DI NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI



Si stabilisce l'obbligo per tutti i Titolari del trattamento di effettuare la notifica della violazione all'autorità di controllo entro 72 ore ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Le figure previste dal GDPR

Titolare del trattamento

- Responsabile dell'applicazione del GDRP
- Sanzioni fino a 20 mln o 4% del fatturato

Responsabile del trattamento

- Incarico con contratto vincolante
- Istruzione documentata
- Assiste il titolare

Persone autorizzate al trattamento

- Esecutori materiali delle attività di trattamento

RPD o DPO

- Responsabile Protezione dati personali (non è il responsabile del trattamento)

OBBLIGO DI NOMINA DELLA FIGURA DEL DPO

Prof. Claudio Pantanali, PhD - cpantanali@units.it

I COMPITI DEL DPO

Informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

Verificare l'attuazione e l'applicazione del Regolamento nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

Fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

Fungere da punto di contatto per gli interessati;

Cooperare e fungere da punto di contatto per l'Autorità di controllo