COORDINAMENTO NAZIONALE ASSOCIAZIONI IMPRENDITORI

GDPR
General Data Protection Regulation

nuovo Regolamento UE
in materia di protezione dei dati personali

VENERDI 8 SETTEMBRE 2017

Formazione Middle Manager
Sviluppo Professionale Responsabili Sedi Territoriali CNAI

Progetto a cura del CNAIForm Associazione per la Formazione
in collaborazione con Centro Studi CNAI

CNAI MEDIADV DESIGN & SERVIZI

comunicazione e grafica del gruppo CNAI

GDPR 679/2016

IL REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il General Data Protection Regulation – in vigore dal 25 maggio 2018
è il nuovo Regolamento Europeo n. 679 del 2016 che riguarda la protezione dei dati per le persone fisiche all'interno dell'Unione Europea.
Sostituisce il "vecchio" Codice Privacy – D. Lgs. 196/2003 – introducendo importanti novità il cui effetto si traduce nel:

- Adeguamento della protezione dati all'evoluzione tecnologica
- Armonizzare la disciplina a livello europeo

GDPR 679/2016

TERRITORIO E INTERESSATI

Il Codice Privacy attualmente in vigore determina il territorio di applicabilità della legge sulla privacy:

a. quando il titolare è stabilito sul suolo italiano

b. pur non essendo stabilito sul territorio italiano, utilizza per il trattamento strumenti situati nel territorio

GDPR 679/2016

TERRITORIO E INTERESSATI

Con il GDPR viene stabilita l'estensione territoriale extra UE dell'applicazione della disciplina europea a determinate condizioni. Art. 3 par. 1**: applicabilità della disciplina**" indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione" applicabile:

- **AZIENDE:** che hanno uno stabilimento nella UE, anche se il trattamento viene fatto extra Unione
- **PERSONE FISICHE (par. 2):** se il trattamento, anche se il titolare non è stabilito nell'Unione, riguarda:
- Offerta di beni/prestazioni nella UE
- Monitoraggio del loro comportamento all'interno della UE

GDPR 679/2016

APPROCCIO AL RISCHIO

Il rischio e la sua valutazione rappresentano il punto focale intorno al quale tessere le fila di una rete di protezione per un trattamento dei dati che garantisca la loro libera circolazione.

Con il nuovo GDPR si passa dal trattamento effettuato applicando le misure MINIME garantite (art. 33 Codice Privacy 196/2003) all'adozione di misure di sicurezza ADEGUATE (art. 24 par. 1 GDPR)

GDPR 679/2016

APPROCCIO AL RISCHIO

Introduzione del nuovo approccio basato sul rischio:

RISK-BASED APPROACH che si traduce ne:

Valutazione dell'Impatto (Privacy Impact Assessment)

Contenuti minimi:

- descrizione sistematica
- valutazione dei rischi
- misure previste per affrontarli

P.I.A. Obbligatoria quando: art. 35 par. 3

a) profilazione

b) dati sensibili e/o giudiziari

c) sorveglianza sistematica su larga scala luogo aperto al pubblico

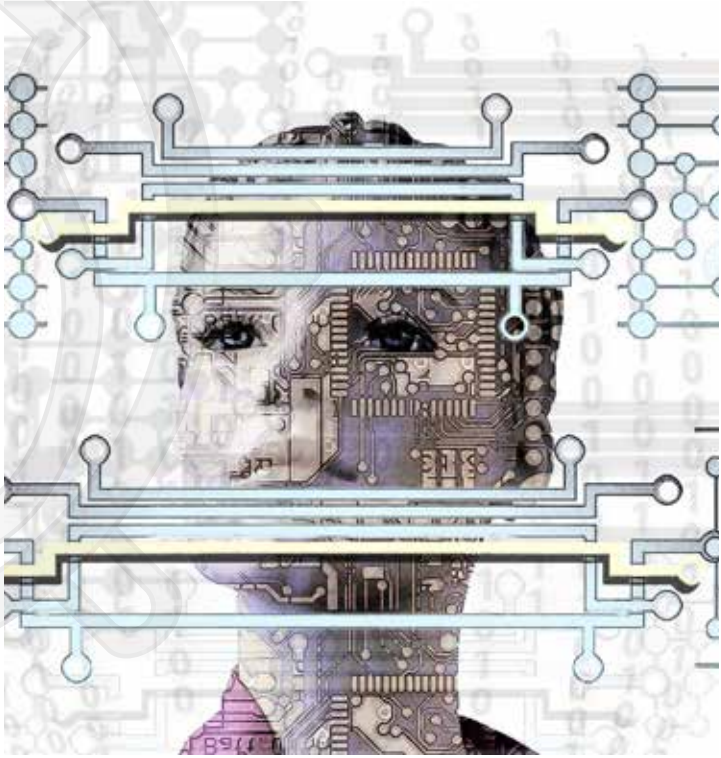
GDPR 679/2016

INFORMATIVA

Per prestare il consenso, la legge impone di conoscere tutto ciò che può essere utile a rendere la scelta conscia, responsabile e dalle conseguenze minime.

Viene abbandonata la complessità – di linguaggio e di significato – imposta dal Codice Privacy 196/2003 per adottare un sistema più snello e funzionale:

art. 12 GDPR: **prevede un'informativa chiara, concisa, trasparente ed intellegibile perl'interessato.**



GDPR 679/2016

INFORMATIVA

ANCHE IN FORMATO ELETTRONICO

art. 13 e 14 GDPR:

elenco tassativo dei contenuti

- dati Responsabile e DPO
- finalità
- strumenti di trasferimento in Paesi Terzo
- periodo conservazione dei dati
- diritto di reclamo
- se il trattamento è soggetto a processi automatizzati

GDPR 679/2016

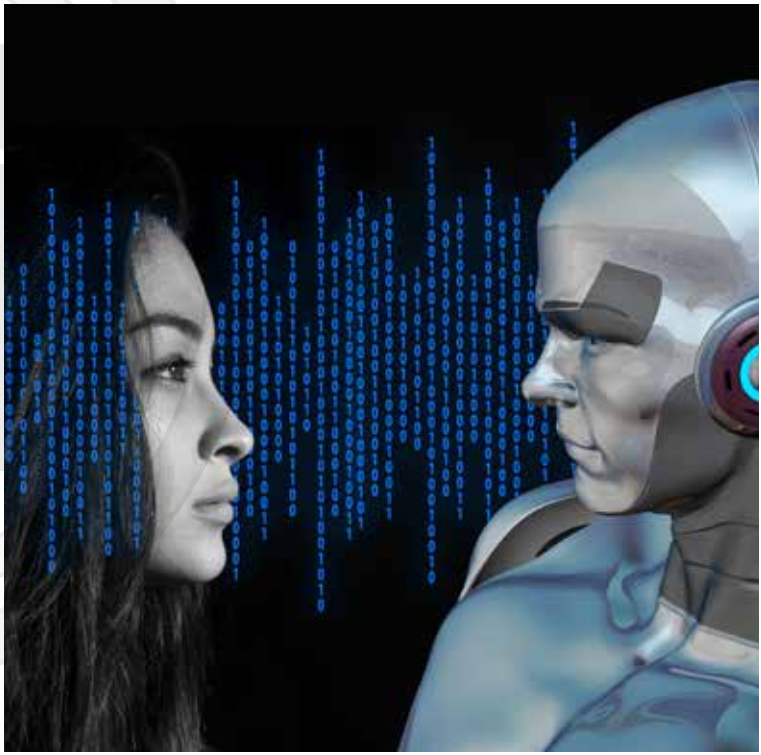
CONSENSO

Se la valutazione del rischio è il punto focale intorno al quale costruire la rete di protezione dei dati, il consenso rappresenta il punto di partenza per avviarne il trattamento.

Art. 7 GDPR: **deve essere dimostrato dal titolare se il consenso è stato prestato.**

Deve essere:

- Preventivo
- Inequivocabile



GDPR 679/2016

CONSENSO

Art. 8 GDPR:

- dai 16 anni in poi il trattamento è lecito
- dai 13 ai 16 anni ci deve essere l'autorizzazione dei genitori
- prima dei 13 anni non può essere prestato consenso

Per i dati sensibili (art. 9 GDPR) **il consenso deve essere esplicito.**

GDPR 679/2016

NUOVI OBBLIGHI E RESPONSABILITÀ

Il nuovo Regolamento ha come fondamento, visto l'obiettivo della sempre più libera ma sicura circolazione dei dati, una tutela "tagliata su misura" per il trattamento da porre in essere.
Così i ruoli e le relative responsabilità evolvono in un assetto meno generico, "cambiando vestito e vestibilità".

GDPR 679/2016

NUOVI OBBLIGHI E RESPONSABILITÀ

1. ACCOUNTABILITY

Art. 5 par. 1 GDPR: **principi su cui deve basarsi il trattamento**

- liceità correttezza e trasparenza
- limitazione delle finalità
- minimizzazione dei dati
- esattezza
- limitazione della conservazione
- integrità e riservatezza

GDPR 679/2016

NUOVI OBBLIGHI E RESPONSABILITÀ

Art. 5 par. 2 GDPR: **il titolare deve rispettare i principi del par. 1 ed è in grado di comprovarlo** (responsabilizzazione = ACCOUNTABILITY) ponendo in atto:

Autovalutazione: per misurare il proprio grado di efficienza ed efficacia nel mettere in atto tutte le misure necessarie

Nuovi principi di protezione:

- privacy by design: adozione di misure in fase di progettazione
- privacy by default: adozione di misure all'atto del trattamento

Strumenti operativi:

- Codici di Condotta (art. 40) per precisare l'applicazione del Regolamento
- Certificazione (art. 42) per rafforzare la credibilità del titolare
- Registro delle Attività (art. 30) obbligatorio per aziende con più di 250 dipendenti

GDPR 679/2016

NUOVI OBBLIGHI E RESPONSABILITÀ

2. DATA BREACH – OBBLIGO DI NOTIFICA IN CASO DI VIOLAZIONE

A CHI?

- **Autorità di controllo**

Elementi della notifica:

- descrizione della natura della violazione
- il nome e i dati del DPO
- descrizione delle probabili conseguenze della violazione
- descrizione delle misure adottate o che si vuole adottare

GDPR 679/2016

NUOVI OBBLIGHI E RESPONSABILITÀ

2. DATA BREACH – OBBLIGO DI NOTIFICA IN CASO DI VIOLAZIONE

A CHI?

- **Interessato** se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche

Elementi della notifica:

- dati identificativi del DPO
- possibili conseguenze violazione
- possibili misure adottate o adottabili

GDPR 679/2016

NUOVI OBBLIGHI E RESPONSABILITÀ

CAUSE DELLE VIOLAZIONI

- preparazione insufficiente
- comportamento colposo/doloso
- entusiasmo – distrazione – curiosità - incertezza

TIPOLOGIE DI VIRUS E TRUFFE ONLINE

GDPR 679/2016

NUOVE MISURE TECNOLOGICHE DI SICUREZZA

L'**Information Technology** corre velocemente e con essa i mezzi utilizzati per dare adeguatezza alle metodologie di trattamento e di protezione dei dati.

DATA GOVERNANCE (art. 32 GDPR):
mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

- La pseudonimizzazione: non attribuzione ad un soggetto specifico dei dati trattati

- La cifratura: modalità di conversione del testo originale in una sequenza di numeri, segni e lettere da decifrare attraverso diverse tecniche (es. Pretty Good Privacy)

GDPR 679/2016

PROTAGONISTI DEL TRATTAMENTO

Restano, come già previsto dal Codice Privacy 196/2003, attori del trattamento e della protezione dei dati anche se con compiti adattati alle nuove esigenze:

Titolare del trattamento: **CHI È?**

- art. 4 par. 7 GDPR: colui che determina le finalità e i mezzi del trattamento
- Art. 24 GDPR: mette in atto misure tecniche e organizzative adeguate

Responsabile del trattamento: **CHI È?**

- art. 4 par. 8 GDPR: colui che tratta dati personali per conto del titolare del trattamento SU ISTRUZIONE DOCUMENTATA DEL TITOLARE

GDPR 679/2016

PROTAGONISTI DEL TRATTAMENTO

RESPONSABILITÀ

Il titolare è responsabile se il suo trattamento viola il regolamento

Il responsabile è responsabile se:

- non ha adempiuto agli obblighi del presente regolamento specificatamente diretti ai responsabili
- ha agito in modo difforme o contrario alle legittime istruzioni del titolare

GDPR 679/2016

PROTAGONISTI DEL TRATTAMENTO

DATA PROTECTION OFFICER

Responsabile della protezione dati:

questa nuova figura, introdotta con il nuovo Regolamento, nasce con l'intenzione del legislatore di favorire l'osservanza della normativa supportando il titolare e svolgendo da interfaccia fra tutti i soggetti coinvolti.

GDPR 679/2016

PROTAGONISTI DEL TRATTAMENTO

DATA PROTECTION OFFICER

a) **Nomina obbligatoria del DPO** (art. 37 par. 1 GDPR) **quando**:

Il trattamento è effettuato da autorità/organismo pubblici

Attività principali del titolare/responsabile consistono in:

- monitoraggio e sistematico su larga scala
- trattamento su larga scala di dati sensibili/giudiziari
- Può essere lavoratore dipendente o autonomo.
- Può essere costituito anche da un TEAM costituito da tutti soggetti qualificati.

GDPR 679/2016

PROTAGONISTI DEL TRATTAMENTO

DATA PROTECTION OFFICER

b) **Posizione del DPO** (art. 38 GDPR):

- Deve essere coinvolto in tutte le attività che riguardano il trattamento

dei dati personali e avere tutte le risorse necessarie per assolvere ai suoi compiti

- Può anche svolgere altri compiti/funzioni evitando conflitto d'interessi
- Riservatezza/segretezza
- Punto di riferimento per gli interessati circa il trattamento dei loro diritti
- Riferisce al vertice del titolare

GDPR 679/2016

PROTAGONISTI DEL TRATTAMENTO

DATA PROTECTION OFFICER

c) **Requisiti**:

- Conoscenze normative
- Familiarità trattamento dati
- Familiarità tecnologie informatiche e sicurezza
- Conoscenza dello specifico settore attività
- Capacità di promuovere la cultura in tema di protezione dati

GDPR 679/2016

PROTAGONISTI DEL TRATTAMENTO

DATA PROCESSOR OFFICER

d) **Compiti** (art. 39 GDPR):

- Informare/consigliare titolare sugli obblighi imposti dal GDPR e altre norme UE
- Sorvegliare sull'osservanza del GDPR
- Fornire un parere sulla Valutazione d'Impatto – se richiesto
- Cooperare con l'autorità di controllo

GDPR 679/2016

DIRITTI DELL'INTERESSATO

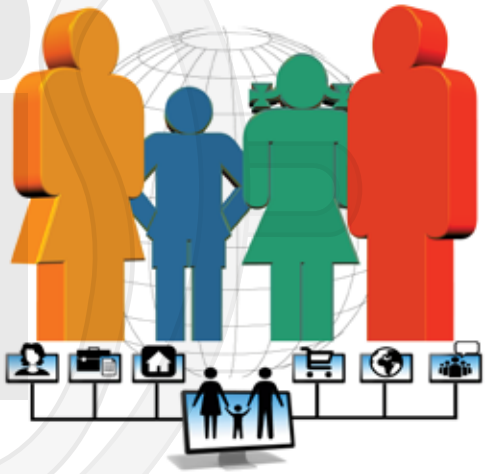
Non solo tutele ma anche nuovi diritti da esercitare per gli interessati.
Tutti viaggiano nello stesso senso: aumentare la libertà di circolazione dei dati assicurandone una sempre maggiore protezione.

GDPR 679/2016

DIRITTI DELL'INTERESSATO

a) **Diritto all'oblio** (art. 17 GDPR): "**il diritto di essere dimenticato**" quando

- non c'è più necessità di raccogliere i dati
- è stato ritirato il consenso
- c'è opposizione al trattamento
- il trattamento è contro il regolamento



Diritto alla **DE-INDICIZZAZIONE**: cancellazione, quando richiesto dall'interessato e possibile da realizzare, dei dati così da evitare il collegamento a tutti i link.

Compresa copia e riproduzione.

GDPR 679/2016

DIRITTI DELL'INTERESSATO

b) **Portabilità dei dati** (art. 20 GDPR):

ricevere dal titolare i dati ad esso forniti in un formato strutturato e trasmetterli ad altri soggetti per il trattamento.

Se:

- I dati sono forniti dall'interessato
- I dati riguardano l'interessato
- Non ledono le libertà/diritti altrui

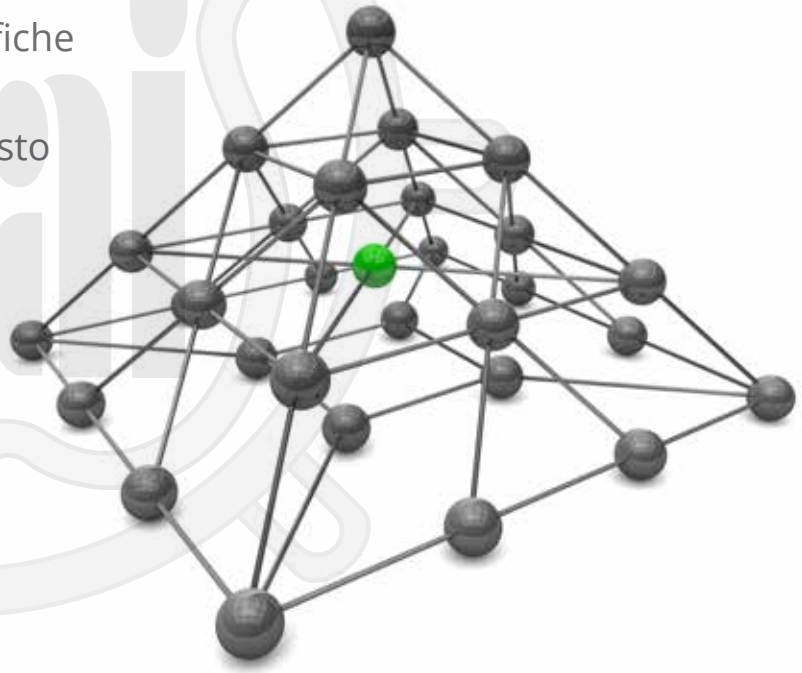
c) Diritto alla rettifica (art. 16 GDPR): se i dati sono incompleti e/o inesatti

GDPR 679/2016

DIRITTI DELL'INTERESSATO

d) **Diritto alla limitazione** (art. 18 GDPR): quando

- Richiesta la rettifica, si è in attesa delle modifiche
- In caso di trattamento illecito, si chiede al posto della cancellazione
- In sede giudiziaria
- In attesa di verifica, in caso di opposizione



GDPR 679/2016

DIRITTI DELL'INTERESSATO

e) **Diritto di opposizione** (art. 21 GDPR):

- in qualunque momento
- particolare situazione dell'interessato
- il titolare deve astenersi dal trattamento

GDPR 679/2016

TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

Il concetto di “confine” oggi è sempre più liquido per non dire trasparente. Se ciò vale in senso materiale, pensiamo al mondo digitale e alla relativa necessità di protezione come di libertà.

GDPR 679/2016

TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

Art. 44 GDPR: Principio di ADEGUATEZZA

Il trasferimento, basato sulla decisione della Commissione, viene concesso solo se garantito un livello di protezione adeguato per il trattamento dei dati.

Il **GDPR** deve essere adottato anche fuori dalle realtà che lo hanno voluto e approvato.

GDPR 679/2016

SISTEMA SANZIONATORIO

Con il nuovo Regolamento c'è un forte inasprimento del sistema sanzionatorio. L'obiettivo, in tema di libertà, è di costituire il deterrente alla disapplicazione della legge e di porre l'attenzione sull'importanza **INDEROGABILE** della circolazione dei dati personali e la relativa protezione al passo con i tempi.

Art. 83 GDPR

La sanzione pecuniaria è fino a

€ 20.000.000,00

o al **4% del fatturato**

GDPR 679/2016

CONCLUSIONI

EFFETTI del GDPR:

per gli **STATI MEMBRI**: circolazione dei dati libera, tutelata e basata su legislazione uniforme.

per le **AZIENDE**: trasparenza, efficienza e competitività

per i C**ONSULENTI**: creare nuove occasioni di crescita e di sviluppo personali e per i propri clienti

COORDINAMENTO NAZIONALE
ASSOCIAZIONI IMPRENDITORI

RELAZIONI SINDACALI

SERVIZI

CENTRO STUDI

CNAI - Coordinamento Nazionale Associazioni Imprenditori

Sede Nazionale

V.le Abruzzo, 225 66100 Chieti Scalo (CH)

Tel. 0871 54 00 93

www.cnai.it - cnai@cnai.it

CNAIForm - Associazione per la Formazione

Tel. 0871 540093 - Fax. 0871 571538

www.cnaiform.it - segreteria@cnaiform.org

www.cnai.it

puoi seguire CNAI su