



Privacy



Corso di Formazione 'Privacy 2.0'

EVOLUZIONE E TUTELA NELLA NORMATIVA EUROPEA

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
REGOLAMENTO UE 2016/679

RELATORE: CLAUDIO AMORUSO

Con il regolamento generale sulla protezione dei dati (Regolamento UE 2016/679) la **Commissione europea** ha inteso rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei suoi confini.

Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016, è entrato in vigore il 25 maggio 2016 ed è efficace dal 25 maggio 2018

Il General data protection regulation è stato appunto armonizzato nel nostro Paese con il decreto n.101 del 10 agosto 2018 pubblicato in Gazzetta Ufficiale il 4 settembre 2018 che entrerà ufficialmente **in vigore dal 19 settembre 2018**

A CHI SI APPLICA

Il regolamento si applica:

- ai dati dei **residenti nell'Unione Europea**;
- a **imprese ed enti, organizzazioni in generale**, con sede legale **fuori dall'UE** che trattano dati personali di **residenti nell'Unione Europea**. Ciò anche **a prescindere** dal luogo o **dai luoghi ove sono collocati i sistemi di archiviazione** (storage) e di elaborazione (server).
- Social network, piattaforme web e motori di ricerca saranno quindi soggetti alla normativa europea anche se sono gestiti da società con sede fuori dall'UE..

Il Regolamento **NON SI APPLICA** ai trattamenti di dati personali:

Effettuati dagli **Stati membri nell'esercizio di attività**;

Effettuati da una **persona fisica** per l'esercizio di attività di **carattere esclusivamente personale o domestico**;

Effettuati dalle **Autorità ai fini di prevenzione, indagine, accertamento** o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguarda contro minacce alla sicurezza pubblica e la prevenzione delle stesse

PRINCIPALI NOVITA' DGPR 679/2016

DATI PERSONALE qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);

sono **qualunque informazione relativa a un individuo**, collegata alla sua vita sia privata, sia professionale o pubblica. Può riguardare qualunque dato personale: nomi, foto, indirizzi e-mail, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer».

I dati personali possono riguardare sia persone fisiche che persone giuridiche.

TITOLARE DEL TRATTAMENTO 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;**

VIOLAZIONE DEI DATI PERSONALI la violazione di sicurezza che comporta **accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

I NUOVI PRINCIPI INTRODOTTI DAL DGPR 679/2016

“**ACCOUNTABILITY**” (artt. 24 e 32)

Il termine anglosassone non è facilmente traducibile e difatti nella traduzione del Regolamento Europeo si parla **impropriamente di “RESPONSABILITÀ”**
La traduzione più corretta potrebbe essere **“RENDICONTAZIONE”**

Che cosa è la rendicontazione? “rendere conto”

Rendicontazione delle spese: è una operazione in base alla quale **si dettaglia** voce per voce **come sono stati spesi dei soldi** (un budget assegnato ad un reparto, un finanziamento pubblico, ecc). La rendicontazione **deve essere supportata da documenti** cartacei che **dimostrano che quelle spese sono state effettivamente sostenute**.

In virtù, difatti, del principio di accountability nel Regolamento dispone che **il titolare del trattamento adotta** politiche **e attua misure adeguate** per **garantire** ed essere **in grado di dimostrare** che il trattamento dei dati personali effettuato è **conforme allo stesso Regolamento**.

Privacy by design e by default (art. 25)

La privacy **by design** richiede che Il Titolare adotti e attui misure tecniche e organizzative **sin dal momento della progettazione** oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati.

La privacy **by default** presuppone invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli **dati personali necessari** per ciascuna **specifica** finalità di **trattamento**.

Valutazione d'impatto sulla protezione dei dati (art. 35)

Quando un determinato trattamento - tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità - può presentare un **rischio (minaccia)** elevato per i **diritti e libertà delle persone fisiche**.

Il Titolare deve effettuare una valutazione d'impatto dello stesso sulla protezione dei dati ("Valutazione d'Impatto").

TITOLARE O RESPONSABILE DEL TRATTAMENTO?

TITOLARE DEL TRATTAMENTO: la persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali;

RESPONSABILE DEL TRATTAMENTO: la persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento.

STUDIO PROFESSIONALE E'	QUANDO	IN CHE MODO	QUALI MISURE DI SICUREZZA
TITOLARE DEL TRATTAMENTO	ANAGRAFICA CLIENTI E FATTURE PROGETTI E DISEGNI TECNICI	INCARICO PROFESSIONALE	NORMALI MISURE DI PROTEZIONE DEI DATI PER EVITARE PERDITA DEL DATO
AUTORIZZATO AL TRATTAMENTO	VISURE CATASTALI ESTREZIONE PLANIMETRIE VISURE IPOTECARIE	ATTO DI DELEGA O INCARICO	NORMALI MISURE DI PROTEZIONE DEI DATI PER EVITARE PERDITA DEL DATO
RESPONSABILE DEL TRATTAMENTO	CTU DEL TRIBUNALE CSE DI CANTIERE CTP	IMPLICITO NEL CONFERIMENTO INCARICO	MISURE DI SICUREZZA ADEGUATE ALLA DELICATEZZA DEL DATO E PER EVITARE LA DIVULGAZIONE

L'INFORMATIVA PRIVACY

Prima = l'informativa era spesso lunga, incomprensibile e con richiami normativi complessi.

Con il Nuovo Regolamento Europeo = l'informativa deve essere **leggibile, comunicativa, accessibile**, concisa e scritta con **linguaggio chiaro e semplice** con un numero limitato di riferimenti normativi.

STUDIO PROFESSIONALE INFORMATIVA PER	INFORMATIVA NECESSARIA	MODALITA' DI TRASMISSIONE	INDICAZIONI
ANAGRAFICA CLIENTI E FATTURE	SI	DIVULGATA O RESA DISPONIBILE ALL'ATTO DELLA RACCOLTA	Deve indicare la raccolta dei dati personali per le sole finalità previste dalla legge
PROGETTI E DISEGNI TECNICI	SI	DIVULGATA O RESA DISPONIBILE ALL'ATTO DELLA RACCOLTA	L'informativa deve indicare l'uso esclusivo per le finalità previste dall'incarico
PUBBLICAZIONE PROGETTI/DISEGNI SU CURRICULA O PAGINE WEB	SI	DIVULGATA O RESA DISPONIBILE	L'informativa deve indicare i tempi di conservazione e utilizzo

IL CONSENSO COME CAMBIA?

Prima = il consenso doveva essere **libero, specifico e informato**. Ci doveva essere un atto formale per accettare il trattamento dei dati.

Con il Nuovo Regolamento Europeo = il consenso deve essere libero, specifico, informato e **inequivocabile**.

Il consenso è valido se la volontà è espressa in modo **NON equivoco**.

STUDIO PROFESSIONALE CONSENSO PER	CONSENSO NECESSARIO	MODALITA' DI TRASMISSIONE	NOTE
ANAGRAFICA CLIENTI E FATTURE	NO	NON APPLICABILE	
PROGETTI E DISEGNI TECNICI	NO	NON APPLICABILE	
PUBBLICAZIONE PROGETTI/DISEGNI SU CURRICULA O PAGINE WEB	SI	Persona fisica identificata o identificabile ?????	Consenso In FORMA SCRITTA ESPLICITO ED INEQUIVOCABILE

RICONOSCIMENTO DI NUOVI DIRITTI

Prima = pochi diritti che tutelavano l'interessato in merito alla gestione dei suoi dati.

Con il Nuovo Regolamento Europeo = nuovi diritti: diritto alla **portabilità** dei dati (posso pretendere che il soggetto a cui ho concesso l'uso dei miei dati me li restituisca su un supporto elettronico strutturato così che io possa farne ulteriore uso, anche presso un altro fornitore), **diritto all'oblio** (vale a dire a essere totalmente dimenticato da chi ha raccolto i miei dati).

STUDIO PROFESSIONALE	DIRITTI DELL'INTERESSATO	SI APPLICA	NON SI APPLICA	NOTE
ANAGRAFICA CLIENTI E FATTURE	PORTABILITA' OBLIO		NON SI APPLICA	L'obbligo legale di conservazione e non può essere sostituito
PROGETTI E DISEGNI TECNICI	PORTABILITA' OBLIO		NON SI APPLICA	
PUBBLICAZIONE PROGETTI/ DISEGNI SU CURRICULA O PAGINE WEB	PORTABILITA' OBLIO	SI APPLICA		Valido solo per la pubblicazione del dato

OBBGLIGO DI SEGNALAZIONE IN CASO DI VIOLAZIONE DEI DATI “Data Breach”

Prima = non era necessario comunicare violazioni nel trattamento dati.

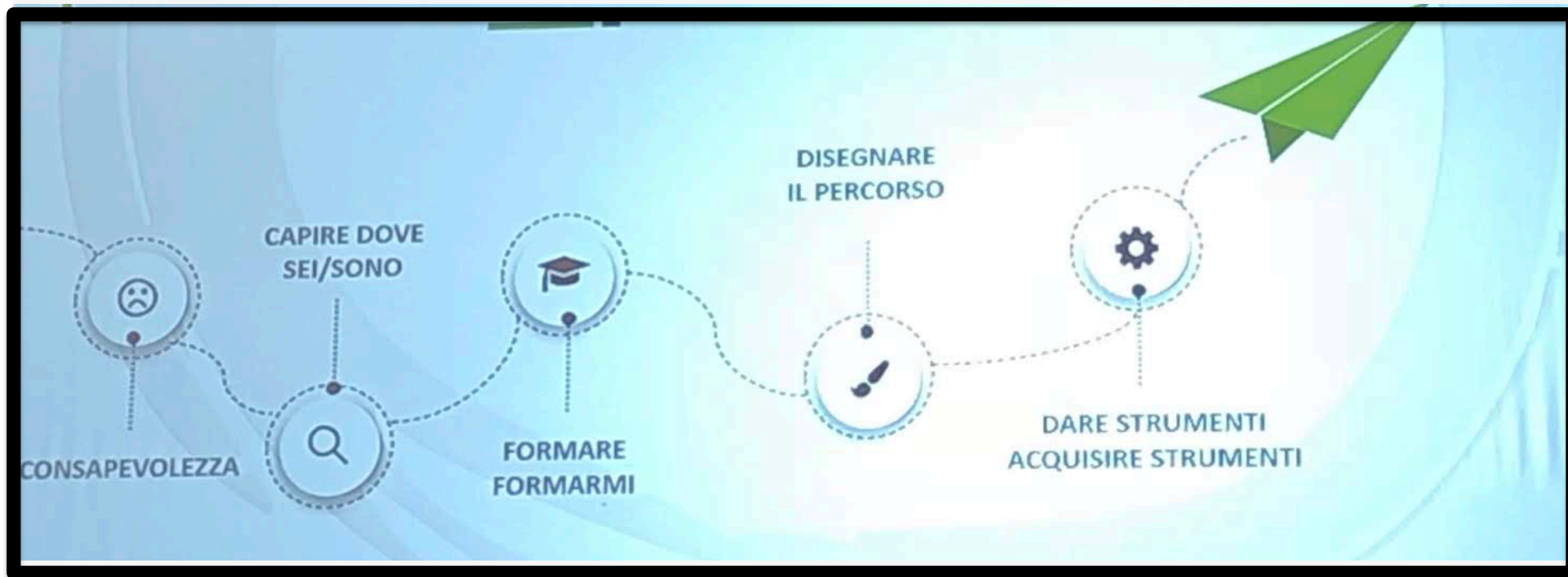
Con il Nuovo Regolamento Europeo = nel caso di violazione del trattamento dati bisogna effettuare una **segnalazione al Garante entro 72 ore** dall'evento e, nel più breve tempo possibile, bisogna informare anche i diretti interessati. Il mancato rispetto di quest'obbligo comporta sanzioni penali.

Stampa Modulo violazione - Data breach

I campi contrassegnati da * sono obbligatori.

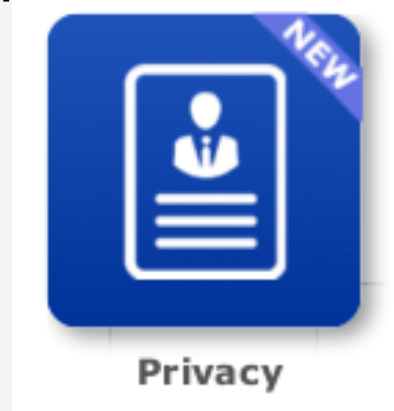
IL DGPR 679/2016 NON PUO' ESSERE UNA SERIE DI ADEMPIMENTI PRECONFENZIONATI

GPDR è un PERCORSO





Applicativo Privacy





GRAZIE PER L'ATTENZIONE!
Contatti help@ufficioweb.com

DEFINIZIONI (art. 4)

1) «**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;

2) «**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;

3) «**limitazione di trattamento**»:

il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «**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;

5) «**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;

6) «**archivio**»:

qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «**titolare del trattamento**»:

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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «**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;

9) «**destinatario**»:

la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «**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;

11)«**consenso dell'interessato**»:

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;

12) «**violazione dei dati personali**»:

la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «**dati genetici**»:

i 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;

14) «**dati biometrici**»:

i 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 facciale o i dati dattiloscopici;

15) «**dati relativi alla salute**»:

i 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;

16) «**stabilimento principale**»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione;

17) «**rappresentante**»:

la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «**impresa**»:

la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «**gruppo imprenditoriale**»:

un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «**norme vincolanti d'impresa**»:

le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

24) «**obiezione pertinente e motivata**»:

un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;



GRAZIE PER L'ATTENZIONE!
Contatti help@ufficioweb.com