



ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI
M I L A N O



Regolamento UE 2016/679 DGPR
Nuovo regolamento europeo sulla protezione dei dati personali

IL NUOVO REGOLAMENTO UE: IL NUOVO VOLTO DELLA PRIVACY

Dott.ssa Turri Michela

Telefono +39 0583 406185

Mobile +39 347 3674033

studio@turriassociati.it

29 gennaio 2018, corso Europa 11 – Milano

REGOLAMENTO 2016/679:

Il Regolamento:

- Pubblicato nella Gazzetta Ufficiale dell'Unione Europea il **4 Maggio 2016**
- Entrato in vigore il ventesimo giorno Successivo alla pubblicazione nella Gazzetta Ufficiale. (**25 Maggio 2016**)
- **Applicabile a decorrere dal 25 Maggio 2018,** giorno in cui sarà ufficialmente abrogata la precedente Direttiva 95/46/CE

Storia della privacy

Oltre vent'anni di storia

**24 ottobre
1995**

Direttiva
96/45/CE:
prima
direttiva
europea in
tema di
tutela e
protezione
dati
personali

**30 giugno
2003**

Decreto
legislativo
196
La «nuova»
legge sulla
Privacy

**9 febbraio
2012,**
decreto

legge n. 5,
convertito,
con
modificazioni
, dalla legge
4
aprile 2012,
n. 35
Abolizione
del
DPS

**25
maggio
2018**
GDPR
pienament
e
attuativo!

**31 dicembre
1996**

Legge 675/96 (la prima
legge sulla privacy) e, in
data 28 luglio 1999,
DPR318/99
(decreto presidenziale
attuativo)

**27 novembre
2008**

Provvedimento
del Garante sugli
Amministratori
di sistema

27 aprile 2016

Approvazione definitiva del
REGOLAMENTO (UE)
2016/679
(pubblicato sulla GU del 4
maggio 2016 entra in
vigore dopo 20 giorni ma
attuativo dal ...

Regolamento i punti focali

- Un regolamento che assicura **uniformità in ambito UE**
- Più attenzione a nuove tecnologie
- Si applica a chi offre servizi/prodotti nell'UE
- Diritto all'oblio
- Data Protection Officer
- Sportello unico ("**one stop shop**") per multinazionali
- Sistema europeo di **sanzioni (uniformi)**

Oggetto e finalità del regolamento privacy (art.1)

Il regolamento mira alla protezione delle **persone fisiche** in materia di trattamento dei dati personali e disciplina la libera circolazione di tali dati.

Il regolamento tutela il **diritto delle persone fisiche alla protezione dei dati personali**

Regolamento ue 2016/679

Ambiti di applicazione

Trattamento automatizzato e non di dati personali,
NON si applica ai trattamenti effettuati:

- Dagli Stati Membri UE in riferimento all'area di Spazio di Libertà, Sicurezza e Giustizia
- Per finalità personale o domestica
- Dalle Autorità per prevenzione, indagine ed esecuzione penale

Regolamento ue 2016/679

Ambito di applicazione territoriale (art. 3)

- Si applica al trattamento dei dati personali nell'ambito delle attività effettuate **da un titolare o responsabile del trattamento nell'Unione**
- Si applica in caso di trattamento dati personali da parte di titolare **non stabilito nell'Unione**, ma in un luogo soggetto al diritto di uno Stato membro

Regolamento ue 2016/679

Ambito di applicazione territoriale (art. 3)

Si applica al trattamento di dati personali di interessati situati nell'UE, effettuati **da titolare o responsabile non stabilito nell'UE**, quando le attività riguardano:

- Offerta di beni o prestazione di servizi agli interessati nell'Unione
- Il monitoraggio del loro comportamento se quest'ultimo ha luogo all'interno dell'Unione

In tal caso, il titolare del trattamento o il responsabile del trattamento non stabilito nell'Ue **dovrà designare un rappresentante nell'Unione** come previsto dall' art. 27.

LICEITÀ DEL TRATTAMENTO (ART. 6)

Il trattamento è lecito se:

- L'interessato ha espresso il proprio consenso al trattamento dei propri dati personali
- Il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte
- Il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;
- Il trattamento è necessario per **salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica**
- Il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
- Il trattamento è necessario per il **perseguimento del legittimo interesse del titolare** del trattamento o di terzi

PRINCIPI DEL NUOVO REGOLAMENTO (ARTT. 5 E 9)

I dati personali devono essere:

- a) Trattati in modo **lecito, corretto e trasparente** nei confronti dell'interessato
- b) Raccolti per **finalità determinate, esplicite e legittime**;
- c) **Adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per le quali sono trattati;
- d) **Esatti e aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle loro finalità
- e) Conservati in maniera da permettere l'identificazione degli interessati per un **periodo non superiore** al conseguimento delle finalità per le quali sono trattati
- f) Trattati in modo da garantire **un'adeguata sicurezza** dei dati personali

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI EXTRA-UE O ORGANIZZAZIONI INTERNAZIONALI

E' lecito solo se il titolare e il responsabile del trattamento rispettano le condizioni del Regolamento:

- Se la Commissione UE ha deciso che il Paese terzo o l'Organizzazione Internazionale garantiscono un livello di protezione adeguato, secondo indici quali: il rispetto dei diritti umani, l'esistenza e la concreta operatività di «autorità garanti», impegni internazionali assunti dal soggetto terzo
- In assenza di quanto sopra, solo se il titolare ha fornito garanzie adeguate (art. 46 Reg. UE) e a condizione che gli interessati dispongano di strumenti giurisdizionali di tutela

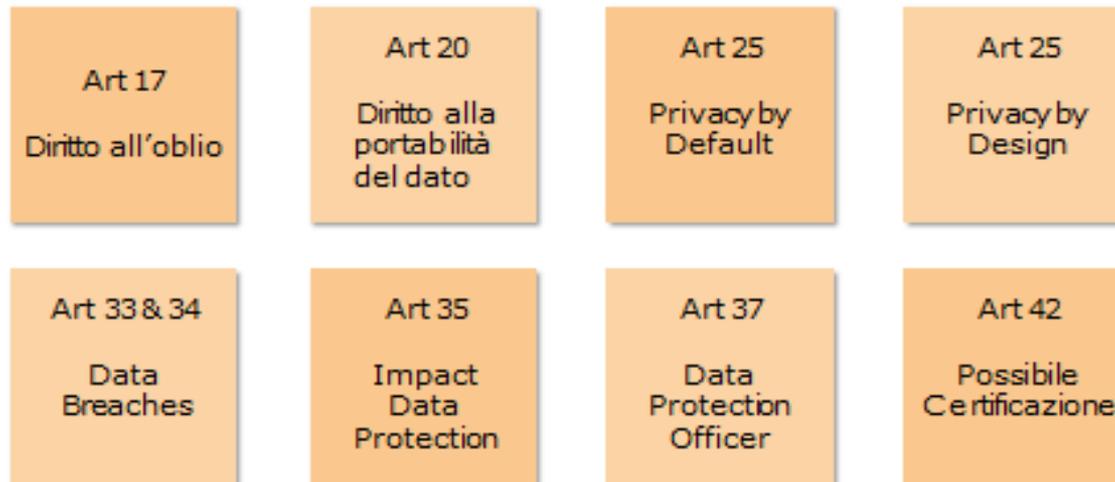
TRASFERIMENTO DI DATI PERSONALI : DEROGHE

- L'interessato abbia prestato consenso esplicito al trasferimento;

- Il trasferimento si rende necessario:
 - all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento
 - per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato
 - per importanti motivi di interesse pubblico
 - per accertare, esercitare o difendere un diritto in sede giudiziaria
 - per tutelare interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità di prestare il consenso

Il nuovo Regolamento Europeo GDPR

Le principali novità

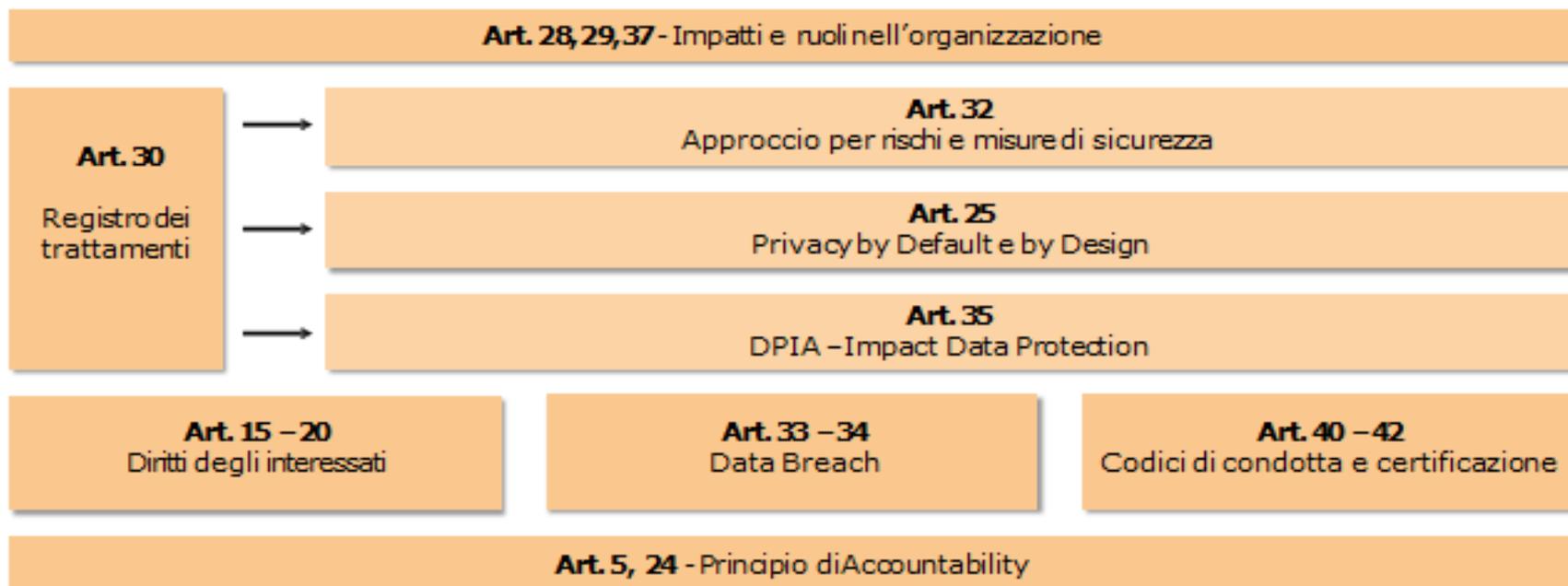


I cambiamenti più importanti possono impattare significativamente sul business.



Il nuovo Regolamento Europeo GDPR

Le principali novità



Il nuovo Regolamento Europeo GDPR

Ruoli ed organizzazione



Articoli
28
29
37

Titolare

Contitolari

Responsabili interni

Responsabili esterni (fornitori UE, extra UE)

Responsabile della Protezione dei Dati (DPO)

Persone autorizzate al trattamento (exIncaricati)

Amministratori di sistema (Prov. Garante 27/11/2008 s.m.i.)

Focus su alcuni ruoli

Principali novità

Responsabilità del titolare

ACCOUNTABILITY

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi a venti probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Responsabilità dei contitolari

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità.

Responsabilità solidale di titolare e responsabile

Il Titolare e il Responsabile del trattamento sono responsabili in solido nei confronti dell'interessato, per un eventuale danno causato dal trattamento.

Designazione di terzi da parte del responsabile del trattamento

Nella nomina di un Responsabile del trattamento, il Titolare potrà prevedere una delega scritta specifica o generale per la designazione di eventuali Responsabili terzi, a fronte dell'obbligo di comunicare ogni nomina effettuata.

Focus su alcuni ruoli

Principali novità

Responsabilità della protezione dei dati

DPO

Figura indipendente nominata dal titolare e dal responsabile del trattamento. Svolge le seguenti funzioni: informare e consigliare il Titolare o il Responsabile in merito agli obblighi del Regolamento, verificarne l'applicazione e l'attuazione, fornire pareri, fungere da punto di contatto sia con gli interessati che con il Garante.

E gli incaricati?

Erano esplicitamente previsti dalla direttiva europea 95/46 e anche dal d.lgs.196/2003. Ora non sono previsti «esplicitamente» sono quindi scomparsi? Assolutamente no. L'art 28 comma 3 dice che il Responsabile (e quindi a maggiore ragione il Titolare) debba garantire «che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza». Quindi gli «incaricati» nella sostanza devono essere individuati e designati con un mandato ancora più forte!

E gli amministratori di Sistema?

Di questi aspetti non si parla esplicitamente nel regolamento Europeo. Gli amministratori di sistema erano stati oggetto di un Provvedimento specifico dell'Autorità garante italiana del 27 novembre 2008 (modificato il 25 giugno 2009). Il provvedimento rimane pienamente in vigore, non smentito dal GDPR. Anzi dal principio di «accountability», il provvedimento esce fuori rafforzato.

Il nuovo regolamento europeo GDPR

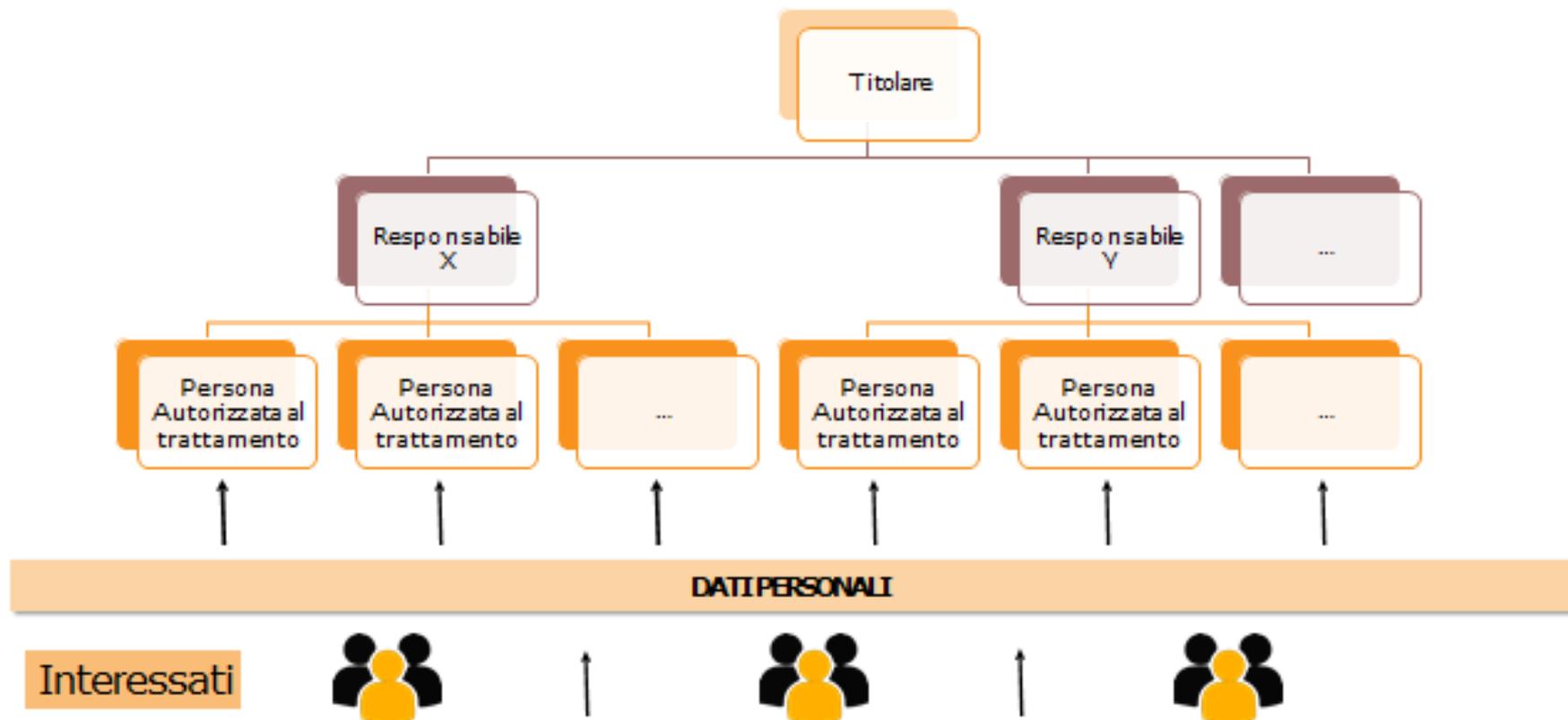
Riassunto degli impatti organizzativi ed operativi



- Identificare, pubblicare e gestire la mappa dei ruoli e delle persone incaricate del trattamento dei dati.
- In alcuni contesti il titolare deve designare il Data Protection Officer.
- Il Titolare e il Responsabile del trattamento sono responsabili in solido nei confronti dell'interessato.
- Nel caso di trattamenti in outsourcing il fornitore si assume un ruolo di responsabilità che deve essere governata.

Comprovare quanto effettivamente fatto, attraverso opportuna documentazione a supporto.

Sintesi delle relazioni fra i vari attori



Una corsa contro il tempo

Dopo l'adozione nell'aprile del 2016 del Regolamento UE 2016/679, meglio conosciuto come GDPR (General Data Protection Regulation, Regolamento generale sulla protezione dei dati), le aziende come la vostra hanno iniziato una vera e propria corsa contro il tempo per garantire la loro conformità prima dell'effettiva entrata in vigore del Regolamento il **25 maggio 2018**, pena il pagamento di pesanti sanzioni e l'avvio di potenziali procedimenti legali. Il compito risulta esteso e particolarmente complesso perché questo Regolamento amplia molto l'ambito della responsabilità rispetto alla direttiva sulla protezione dei dati del 1995 (Direttiva 95/46/CE) precedentemente in vigore.

C'è però una buona notizia: **non siete soli!** Nelle gare ciclistiche si forma il "gruppo" e per le aziende avviene la stessa cosa: molte di loro si trovano allo stesso punto nel processo di conformità e raggiungeranno il traguardo più facilmente e velocemente grazie alla collaborazione.



Il Regolamento
generale sulla
protezione
dei dati
entra in vigore
25 maggio 2018



Chi partecipa alla corsa?

Le organizzazioni che raccolgono, memorizzano e/o elaborano informazioni personali devono garantire la conformità al GDPR se:

- offrono beni o servizi a cittadini UE residenti nell'UE OPPURE
- monitorano il comportamento di cittadini UE residenti nell'UE.

Sono incluse le organizzazioni che non hanno sede all'interno dell'UE, che non sono presenti in UE sotto nessuna forma e anche quelle con dipendenti UE ma senza clienti UE. Insomma, se gestite in qualche modo informazioni personali che riguardano cittadini UE per beneficio di legge... il GDPR riguarda anche voi!

Tutte le organizzazioni che soddisfano questi criteri devono garantire la conformità. Se elaborate una grande quantità di dati avrete da rispettare un insieme di richieste maggiori.

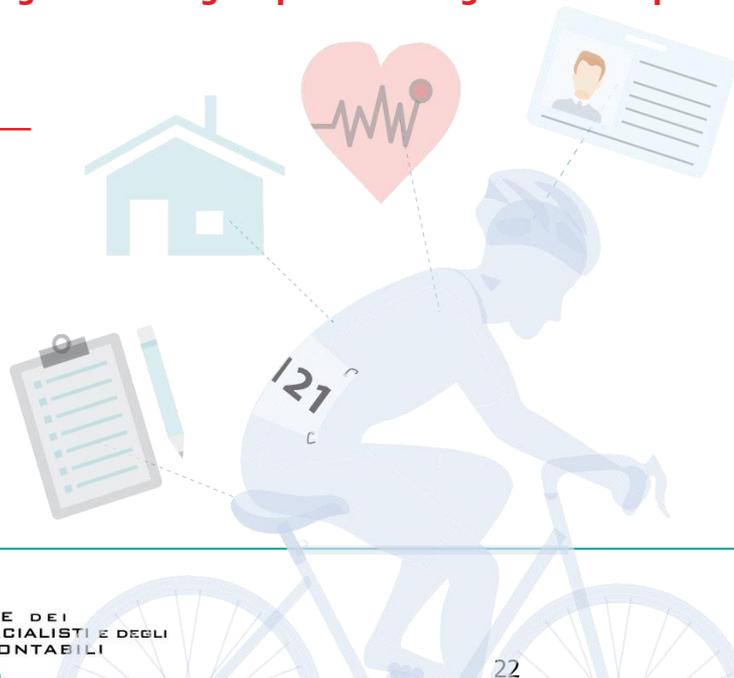
Il Regolamento fa riferimento a organizzazioni che devono garantire la conformità al GDPR in qualità di "titolari del trattamento" o "responsabili del trattamento". I titolari del trattamento sono le entità che determinano le finalità, le condizioni e i mezzi per l'elaborazione dei dati personali, mentre i responsabili del trattamento sono le entità che elaborano i dati personali per conto dei titolari.

Prendiamo, ad esempio, una clinica sanitaria che esternalizza le analisi di laboratorio a un'altra struttura. La clinica avrà bisogno di condividere un certo quantitativo di informazioni personali raccolte con la struttura incaricata delle analisi, per poter restituire ai pazienti i risultati corretti. In questo caso, la clinica sanitaria è il titolare del trattamento dei dati, mentre il fornitore del servizio di analisi è il responsabile del trattamento ai fini del GDPR. Per ognuno di questi ruoli, vi sono differenze nei requisiti del Regolamento, quindi è opportuno stabilire quale spetta alla vostra organizzazione (uno dei due o entrambi).

Cosa si intende per dati personali?

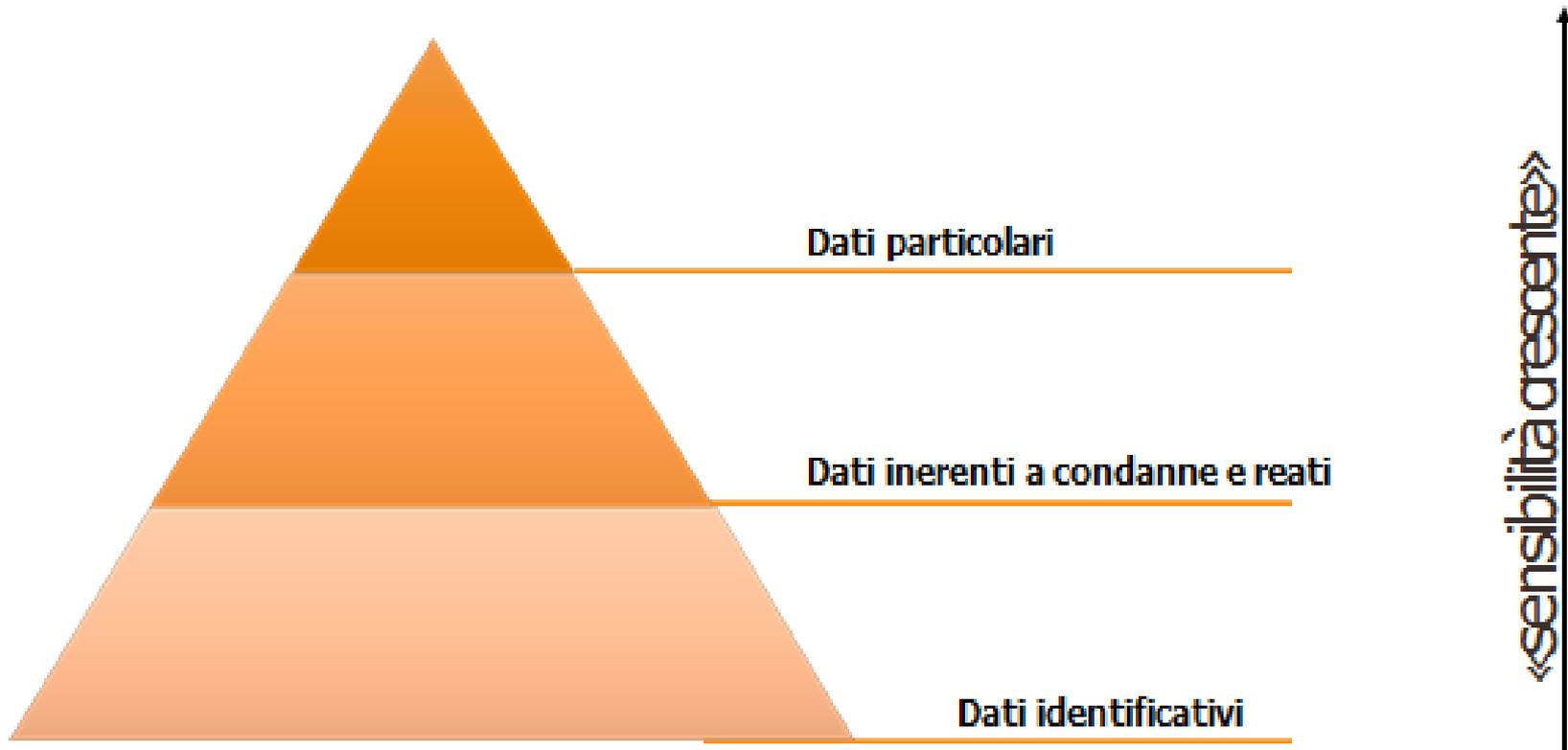
Il GDPR interpreta la definizione di dati personali in senso lato. Qualsiasi informazione che può essere utilizzata per identificare una persona in modo diretto o indiretto deve essere considerata un dato personale. Può trattarsi di un nomi, foto, indirizzi e-mail, coordinate bancarie, numeri di documenti di identità, post su siti web di social network, informazioni mediche e persino indirizzi IP associati a un account o un dispositivo specifico di un utente.

Per fare un esempio, se foste gli organizzatori di una gara e doveste inserire o assegnare i numeri di pettorale in un sistema informatico (dove ogni numero corrisponde a un singolo individuo), tali numeri sarebbero considerati dati personali. Spesso infatti sono facilmente correlabili ad altri dati personali come il nome dell'iscritto, l'indirizzo, la foto, screening medici eseguiti prima della gara e altri tipi di informazioni.



Trattamenti di dati personali

Quali dati?



Classificazione dei dati personali

Dato personale

(Art. 4 comma 1)

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.

Dati personali particolari

(Art. 9 comma 1)

Sono dati particolari: 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.

Altri dati personali particolarmente significativi

(Art. 10)

Dati personali relativi a condanne penali e ai reati.

Gdpr e siti web

La novità nel GDPR è una visione più ampia delle attuali leggi europee sulla privacy:

- **IDs**
- **Indirizzi IP**
- **Geo localizzazione**
- **E altri dati da cookie**

Sono dati personali (PII) e devono essere trattati nello stesso modo in cui si trattano dati come nomi, codici fiscali, dati sanitari, ecc.

Come i cookies sono presenti nei siti

- I cookies sono una delle tecnologie più diffuse se nei siti web
- I siti web sono costruiti da tanti “pezzi digitali” come tanti Mattoncini Lego
- Ogni mattoncino contiene il codice creato da differenti sviluppatori
- Ogni mattoncino può contenere un cookie che manda e riceve dati da e a altri (“terze parti”) per tracciare gli utenti

Come il gdpr impatta i siti web: le nuove responsabilità per i gestori dei siti

- I dati personali non possono essere tracciati o usati prima che l'utente abbia dato il consenso
- Devono essere specificati tutti i tracciamenti dei dati personali per tutte le pagine/URLs
- I visitatori devono essere informati su:
 - Chi riceve i loro dati e come sono usati
 - La data di scadenza del cookie
- Ogni autorizzazione deve essere salvata/registrata per provare alle autorità che è stata data (Formato della prova)
- La negazione del consenso deve essere facile da fare, anche in un secondo momento

Gestione cookie: legge attuale vs gdpr

	Attuale legge italiana (Prov. 229/2014)			GDPR dal 25 maggio 2018		
	Cookie banner	Blocco prima del consenso	Formato della prova	Cookie banner	Blocco prima del consenso	Formato della prova
Solo cookie tecnici/funzionali <i>(shopping cart, selezione lingua, preferenze)</i>	NO	NO	NO	NO	NO	NO
Cookie di statistica di prima parte <i>(es. Piwik e simili)</i>	NO	NO	NO	NO	NO	NO
Cookie di statistica di terza parte con IP anonimizzato <i>(es Analytics)</i>	NO	NO	NO	NO (*) (* dipende dal metodo di anonimizzazione)	NO (*)	NO(*)
Cookie pubblicitari <i>(Google Adsense, DoubleClick, retargeting, ecc)</i>	SI	SI	NO	SI	SI	SI
Altri cookie di terze parti <i>(Social network, YouTube...)</i>	SI	?	NO	SI	SI	SI
Qualsiasi attività di profilazione <i>(include la cross condivisione dei dati da Analytics a altri prodotti Google altre profilazioni di terze parti)</i>	SI + notifica Garante	SI + notifica Garante	NO	SI	SI	SI
Cookie policy	List di tutti i cookie con link alle privacy policies delle terze parti con opzione per opt out. Se i cookie di terze parti sono difficili da identificare, inserire un link a youronlinechoices.com/it .			Lista di tutti i cookie e per ciascuno: - chi riceve i dati e per cosa sono utilizzati; - la data di scadenza.		

Software per gestione del gdpr

- Risolve tutti gli aspetti della conformità dei siti web:
 - **Scannerizza** il tuo sito e la nostra tecnologia identifica più cookie di quanti possano fare altri software
 - Non viene tracciata o inviata nessuna informazione dei dati personali prima che l'utente abbia dato il consenso (**blocco preventivo**)
 - L'utente può **revocare** il consenso in ogni momento
 - Tutti I consensi sono **registrati** in sicurezza per un potenziale audit (formato della prova)
 - Ti offre una base per il DPIA assessment e per i web audits

Come funziona?

- Prima scansione in base al database del software - i cookies vengono identificati i cookie e creati i banner e la informativa
- I testi dei banner e della informativa sono modificabili così come la descrizione e la tipologia dei cookies
- L'informativa può essere integrata in qualsiasi pagina (es. quella della privacy) e riporta anche lo stato attuale del consenso espresso dall'utente con opzione di opt out
- Ogni mese viene fatta una nuova scansione
- Aggiornamento automatico del banner della informativa e report per email

Tale software fornisce una soluzione completa che permette agli imprenditori di:

- Evitare un potenziale problema legale
- Avere un aiuto per i controlli legali
- Avere un notevole risparmio in termini di denaro e tempo

Le autorità di controllo indipendenti

Ogni Stato membro dispone che **una o più autorità pubbliche indipendenti** siano incaricate di sorvegliare l'applicazione del Regolamento privacy **in modo da tutelare i diritti e le libertà fondamentali delle persone fisiche** con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione Europea.

Funzioni delle autorità di controllo

Ogni autorità agisce in piena **INDIPENDENZA** e **TRASPARENZA**.

- Vigilanza
- controllo (può richiedere documenti ed informazioni, disporre accessi, ispezioni e verifiche)
- funzioni giurisdizionali (esamina i reclami e le segnalazioni e decide sui ricorsi presentati dagli interessati)
- funzioni sanzionatorie (Garante è ai sensi dell'art. 162, secondo comma del Codice della privacy organo competente ad irrogare sanzioni amministrative)
- funzioni consultive
- funzione di promozione di iniziative legislative
- funzione sensibilizzazione in materia di protezione dei dati personali
- funzioni di cooperazione internazionale

Compiti delle autorità di controllo

- a) **Controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico**
- b) Esaminare **i reclami e le segnalazioni** e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano
- c) **Prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune** al fine di rendere il trattamento conforme alle disposizioni vigenti
- d) **Vietare anche d'ufficio, in tutto o in parte, il trattamento illecito** o non corretto dei dati o disporre il blocco, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali

Compiti delle autorità di controllo

- e) **Promuovere la sottoscrizione di codici**
- f) **Segnalare al Parlamento e al Governo l'opportunità di interventi normativi**
- g) **Esprimere pareri nei casi previsti**
- h) **Curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati**
- i) **Denunciare i fatti configurabili come reati perseguibili d'ufficio**, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni
- l) Tenere il registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37;
- m) predisporre **annualmente una relazione sull'attività svolta** e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce