Università di Roma Tor Vergata

CREG Centro di Ricerche Economiche e Giuridiche

www.creg.uniroma2.it

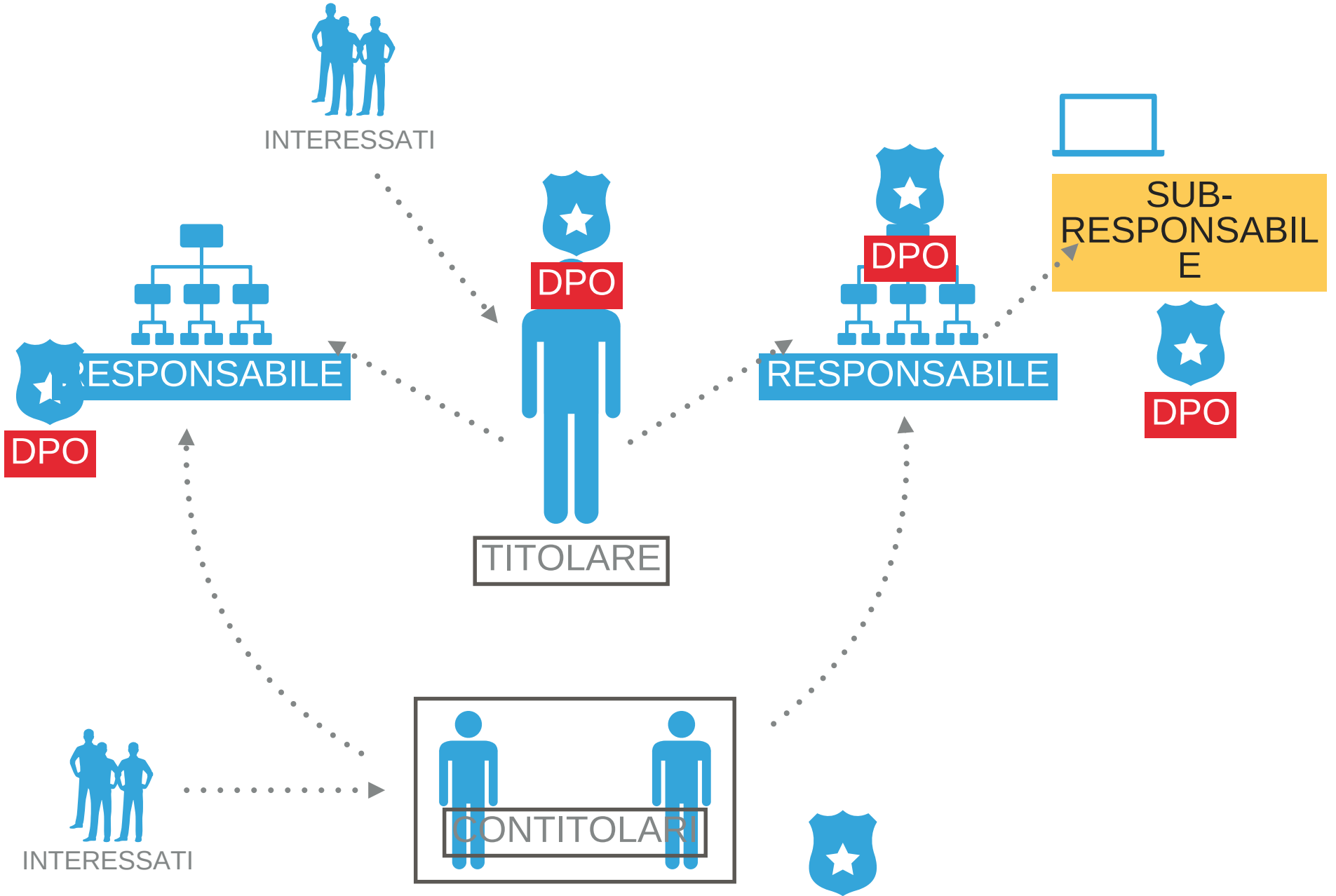
Le nuove figure privacy


privacy
information
personal
protection
internet
data
law
policy
right
rights
people
identity
government
private
secret
social
online
individuals
public
human
users
act
location
technologies
control
protect
market
legal
sites
invasion
freedom
disclosure
use

Il **Regolamento UE 2016/679 (GDPR)**, stabilisce il **principio dell'*accountability***, che può essere definito come responsabilizzazione e dovere di rendicontazione: i soggetti dell'organigramma priva devono assumere un comportamento responsabile, volto a garantire il pieno rispetto di tutti i principi e le norme del Regolamento stesso, nonché essere anche in grado di "comprovarlo".

Il termine *accountability* prevede l'adozione di un **adeguato modello di organizzazione** della struttura preposta al trattamento dei dati personali, che nello schema del GDPR si configura in **3 figure fondamentali**.

I RUOLI DELLE VARIE FIGURE



TITOLARE DEL TRATTAMENTO

Stabilisce le finalità e le modalità del trattamento dei dati personali. Quindi, l'impresa/organizzazione decide «perché» e «come» devono essere trattati i dati personali, è titolare del trattamento. I dipendenti che trattano i dati personali all'interno della tua organizzazione lo fanno per adempiere ai compiti di titolare del trattamento della tua azienda/organizzazione.
L'azienda/organizzazione è contitolare del trattamento quando insieme a una o più organizzazioni definisce congiuntamente «perché» e «come» devono essere trattati i dati personali. I contitolari del trattamento devono stipulare un accordo che definisca le rispettive responsabilità per quanto riguarda il rispetto delle norme del GDPR. Gli aspetti principali dell'accordo devono essere comunicati alle persone i cui dati sono oggetto di trattamento.

RESPONSABILE DEL TRATTAMENTO

Il responsabile del trattamento tratta i dati personali solo per conto del titolare del trattamento. Il responsabile del trattamento è di solito un terzo esterno all'azienda. Tuttavia, nel caso di gruppi di imprese, un'impresa può agire in qualità di responsabile del trattamento per un'altra impresa.

TITOLARE E RESPONSABILE DEL TRATTAMENTO

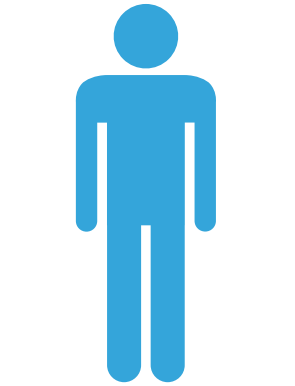
Titolare del trattamento e responsabile del trattamento

Un birrificio ha molti dipendenti. Firma un contratto con una società addetta all'elaborazione delle buste paga per pagare gli stipendi. Il birrificio indica a tale società quando deve essere pagato lo stipendio, quando un dipendente lascia l'azienda o ottiene un aumento di stipendio, e fornisce tutti gli altri dati per le buste paga e i pagamenti. La società fornisce il sistema informatico e conserva i dati dei dipendenti. Il birrificio è il titolare del trattamento e la società addetta all'elaborazione delle buste paga è il responsabile del trattamento.

CONTITOLARI DEL TRATTAMENTO

Contitolari del trattamento

La tua azienda/organizzazione offre servizi di babysitting tramite una piattaforma online. Allo stesso tempo, la tua azienda/organizzazione ha un contratto con un'altra azienda che consente di offrire servizi a valore aggiunto. Questi servizi includono la possibilità per i genitori non solo di scegliere la baby-sitter, ma anche di noleggiare giochi e DVD che la baby-sitter può portare con sé. Entrambe le aziende sono coinvolte nella configurazione del sito web. In questo caso, le due aziende hanno deciso di utilizzare la piattaforma per entrambi gli scopi (servizi di babysitting e noleggio di DVD/giochi) e molto spesso condividono i nominativi dei clienti. Pertanto, le due aziende sono contitolari del trattamento perché non solo accettano di offrire la possibilità di «servizi combinati», ma progettano e utilizzano anche una piattaforma comune.



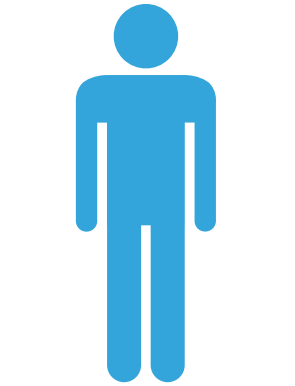
TITOLARE

- PERSONA FISICA
- PERSONA GIURIDICA
- AUTORITA' PUBBLICA
- SERVIZIO
- ALTRO ORGANISMO

DETERMINA LE FINALITÀ E I MEZZI DEL TRATTAMENTO DI DATI PERSONALI

PERCHE’ } AVVIENE IL TRATTAMENTO

COME }



TITOLARE

ACCOUNTABILITY

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**

- NATURA
- FINALITÀ
- CONTESTO
- AMBITO DI APPLICAZIONE
- RISCHI AVENTI PROBABILITÀ E GRAVITÀ DIVERSE PER I DIRITTI E LE LIBERTÀ

SISTEMA DI GESTIONE PRIVACY

PROCEDURE INFORMATIVE

SICUREZZA

CONSENSI

PRIVACY BY DESIGN

NOMINA DPO

ESERCIZIO DEI DIRITTI

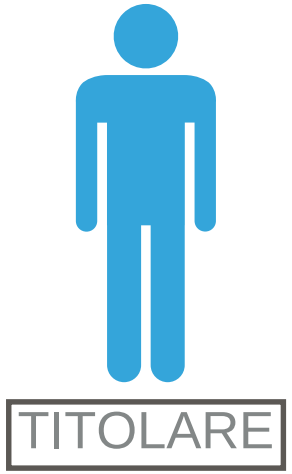
PRIVACY BY DEFAULT

CERTIFICAZIONI

REGISTRO

DPIA

CODICI



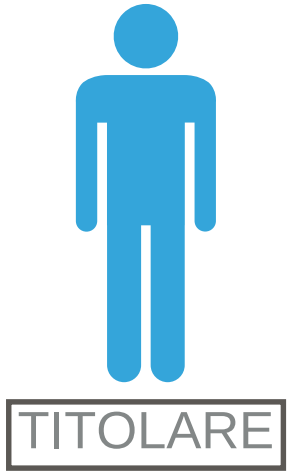
FORMA

In caso di **ente collettivo** (società, pubblica amministrazione, organismo, etc.) il Titolare del trattamento è la **persona giuridica**

In caso di organo di gestione pluripersonale è opportuno individuare **un amministratore** che abbia le **deleghe per attuare quanto previsto dalla normativa**

L'INFORMATIVA DEVE CONTENERE IDENTITÀ E DATI DI CONTATTO DEL TITOLARE DEL TRATTAMENTO

SE SOGGETTO EXTRA-UE NOMINA UN RAPPRESENTANTE NEL TERRITORIO DELLA UE



RESPONSABILITA

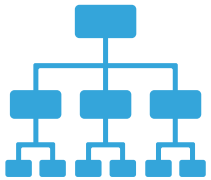
Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal **suo trattamento che violi il regolamento**

Il titolare del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso **non gli è in alcun modo imputabile**

DISCIPLINA ANALOGA A QUELLA ATTUALE CHE PREVEDE RESPONSABILITÀ OGGETTIVA

PROCESSUALMENTE SIGNIFICA INVERSIONE DELL'ONERE DELLA PROVA

I RUOLI DELLE VARIE FIGURE



RESPONSABILE

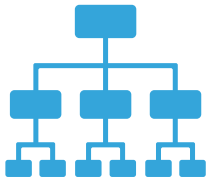
- PERSONA FISICA
- PERSONA GIURIDICA
- AUTORITA' PUBBLICA
- SERVIZIO
- ALTRO ORGANISMO

TRATTA DATI PERSONALI PER CONTO DEL TITOLARE DEL TRATTAMENTO

REQUISITI:

- Prestare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate
- affinché il trattamento sia conforme al regolamento e garantisca la tutela dei diritti dell'interessato

CONOSCENZA SPECIALISTICA, AFFIDABILITÀ E RISORSE, PER METTERE IN ATTO MISURE TECNICHE E ORGANIZZATIVE CHE SODDISFINO I REQUISITI DEL REGOLAMENTO, ANCHE PER LA SICUREZZA DEL TRATTAMENTO



RESPONSABILE

FORMA

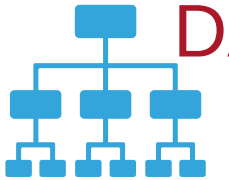
Contratto o altro **atto** giuridicamente vincolante redatto in **forma scritta** anche **in formato elettronico**

CONTENUTO:

vincola il responsabile del trattamento al titolare del trattamento e regola la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento

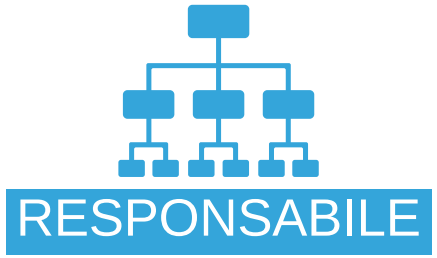
DATA PROCESSING AGREEMENT (DPA)

SULLA CUI BASE IL RESPONSABILE



RESPONSABILE

- tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale
- garantisce che le persone autorizzate si siano impegnate alla riservatezza o abbiano un obbligo legale di riservatezza
- adotta tutte le misure di sicurezza richieste
- rispetta le regole per la nomina di sub-responsabili
- assiste il titolare del trattamento con misure tecniche e organizzative adeguate per esercizio diritti interessati
- assiste il titolare del trattamento per il rispetto degli obblighi sicurezza compresa data breach e DPIA
- cancella o restituisce al Titolare tutti i dati personali e cancella le copie esistenti
- mette a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi
- consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzati dal titolare o da un altro soggetto da questi incari



RESPONSABILITA

Se viola il regolamento **determinando le finalità e i mezzi del trattamento**, è considerato un **titolare** del trattamento in questione.

Se agisce da Responsabile ma viola il GDPR si applica il **medesimo criterio di responsabilità oggettiva** previsto per il Titolare

Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del GDPR specificatamente diretti ai responsabili del trattamento o ha agito in modo **difforme o contrario** rispetto alle legittime **istruzioni** del titolare del trattamento.

E’ PREVISTA UNA RESPONSABILITÀ SOLIDALE TRA TITOLARE E RESPONSABILE (O TRA PIÙ TITOLARI O PIÙ RESPONSABILI)

SUB-RESPONSABILE

EFFETTUA PARTE DEI TRATTAMENTI

PREVIA AUTORIZZAZIONE SCRITTA

particolare o generale da parte del Titolare

SE È GENERALE IL RESPONSABILE DEVE AVVISARE IL TITOLARE DELLE MODIFICHE PER CONSENTIRGLI DI OPPORSI

LA NOMINA DI UN SUB-RESPONSABILE DEVE ESSERE FATTA CON LE MEDESIME FORME PREVISTE PER QUELLA DEL RESPONSABILE E DEVE PREVEDERE IL RISPETTO DEGLI OBBLIGHI ASSUNTI DAL RESPONSABILE VERSO IL TITOLARE

SE IL SUB-RESPONSABILE OMETTE DI ADEMPIERE AI PROPRI OBBLIGHI IN MATERIA DI PROTEZIONE DEI DATI, IL RESPONSABILE INIZIALE CONSERVA NEI CONFRONTI DEL TITOLARE DEL TRATTAMENTO L'INTERA RESPONSABILITÀ

I RUOLI DELLE VARIE FIGURE

DPO DI GRUPPO

Purché sia facilmente raggiungibile da ciascuno stabilimento

DPO UNICO PER PIÙ P.A.

tenuto conto di struttura organizzativa e dimensione

QUANDO

- trattamento da pubbliche amministrazioni
- monitoraggio regolare e sistematico su larga scala
- trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali

CHI

- in funzione delle **qualità professionali,** in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39
- può essere un **dipendente** del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un **contratto di servizi**
- Il responsabile della protezione dei dati **può svolgere altri compiti e funzioni** purché non vi sia **conflitto di interessi**
- riferisce direttamente al **vertice gerarchico**
- deve avere **risorse necessarie** per assolvere i compiti e **accedere** ai dati personali ed ai trattamenti

I DATI DI CONTATTO DEL DPO DEVONO ESSERE INSERITE NELLE INFORMATIVE E COMUNICATI AL GARANTE

COMPITI

- 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 e delle leggi nonché delle politiche del titolare del trattamento o del responsabile del trattamento, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo
- fornire un **parere** in merito alla **DPIA** e **sorvegliarne** lo svolgimento
- **cooperare** con l'autorità di controllo
- fungere da **punto di contatto** per l'autorità di controllo

IL DPO NON HA RESPONSABILITÀ VERSO L'ESTERNO, MA RISPONDE PER RESPONSABILITÀ PROFESSIONALE NEI CONFRONTI DEL TITOLARE O DEL RESPONSABILE

Disposizioni come la limitazione del trattamento o il divieto di trattamento può comportare un danno economico ben più grave rispetto a quello che si potrebbe avere dalla semplice sanzione amministrativa.

Basti pensare che se l'attività di un'azienda è improntata su un determinato trattamento e questo viene vietato come risultato si otterrebbe la chiusura dell'azienda stessa.

Inoltre ogni stato membro può stabilire, entro il 25 Maggio 2018, ulteriori sanzioni come ad esempio la responsabilità civile e penale.

In Italia ad oggi è prevista la responsabilità civile per "Mancata adozione delle misure idonee ad evitare il danno" (art. 15, art. 2050 codice civile), salvo si dimostri di aver adottato le misure idonee ad evitarlo (inversione della prova).

Inoltre sono previste sanzioni penali che, a seconda della tipologia di reato commesso possono prevedere da 6 a 36 mesi di reclusione, tra questi per esempio vi è il "Trattamento illecito di dati".

Un'azienda quindi che diffonde dati dei propri utenti, per esempio mediante l'utilizzo di gruppi WhatsApp o Mailing List in chiaro, o, come capita spesso nei bar lasciando a disposizione un libro per inserire la propria mail per l'invio del menù del giorno senza fornire idonea informativa privacy e senza aver precedentemente chiesto il consenso, può potenzialmente incorrere in questa fattispecie di reato in quanto potrebbe essere dimostrato che da tale utilizzo ne potrebbe trarre profitto.

Articolo 4, punti 7 e 8, e articoli 24, 26, 28 e 29; considerando 74, 79 e 81 del regolamento.

Gruppo di lavoro ex articolo 29 — Parere 1/2010 sui concetti di «titolare del trattamento» e «responsabile del trattamento» (WP 169).

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_it

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597

Regolamento UE 679/2016

https://www.cyberlaws.it/2018/bozza-nuovo-codice-privacy-2018/

https://www.cyberlaws.it/2018/la-bozza-del-decreto-attuativo-del-gdpr/

Grazie per la cortese attenzione