UNIMORE Dipartimento di Economia Marco Biagi
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Fondazione Marco Biagi

I nuovi sviluppi nei ruoli e nelle responsabilità del titolare e del responsabile del trattamento dei dati: le *best practices* nella negoziazione dei termini e delle condizioni delle relazioni controller-to-controller e controller-to-processor

Veronica Palladini - Phd candidate in Lavoro, sviluppo, innovazione, Università di Modena e Reggio Emilia- Fondazione Marco Biagi

28 aprile 2022

IL TITOLARE DEL TRATTAMENTO

Art. 4, par 1, n. 7 del GDPR il titolare del trattamento è 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.

Il Titolare non può essere nominato, è **uno stato di fatto**;

Con «persona fisica»:

a) si allude a coloro che effettuano un trattamento di dati personali nell'ambito della propria **attività commerciale o professionale**, **escludendo** perciò il trattamento dei dati nell'ambito **domestico o esclusivamente personale;**

b) non ci si riferisce alle persone fisiche che operano nella relativa struttura o che sono legittimati a manifestare la volontà dell'ente all'esterno (ad esempio: il direttore generale, il presidente, il legale rappresentante, ecc.) che al più, in un'ottica di **organizzazione delle risorse** saranno considerate designate o autorizzate al trattamento dei dati personali.

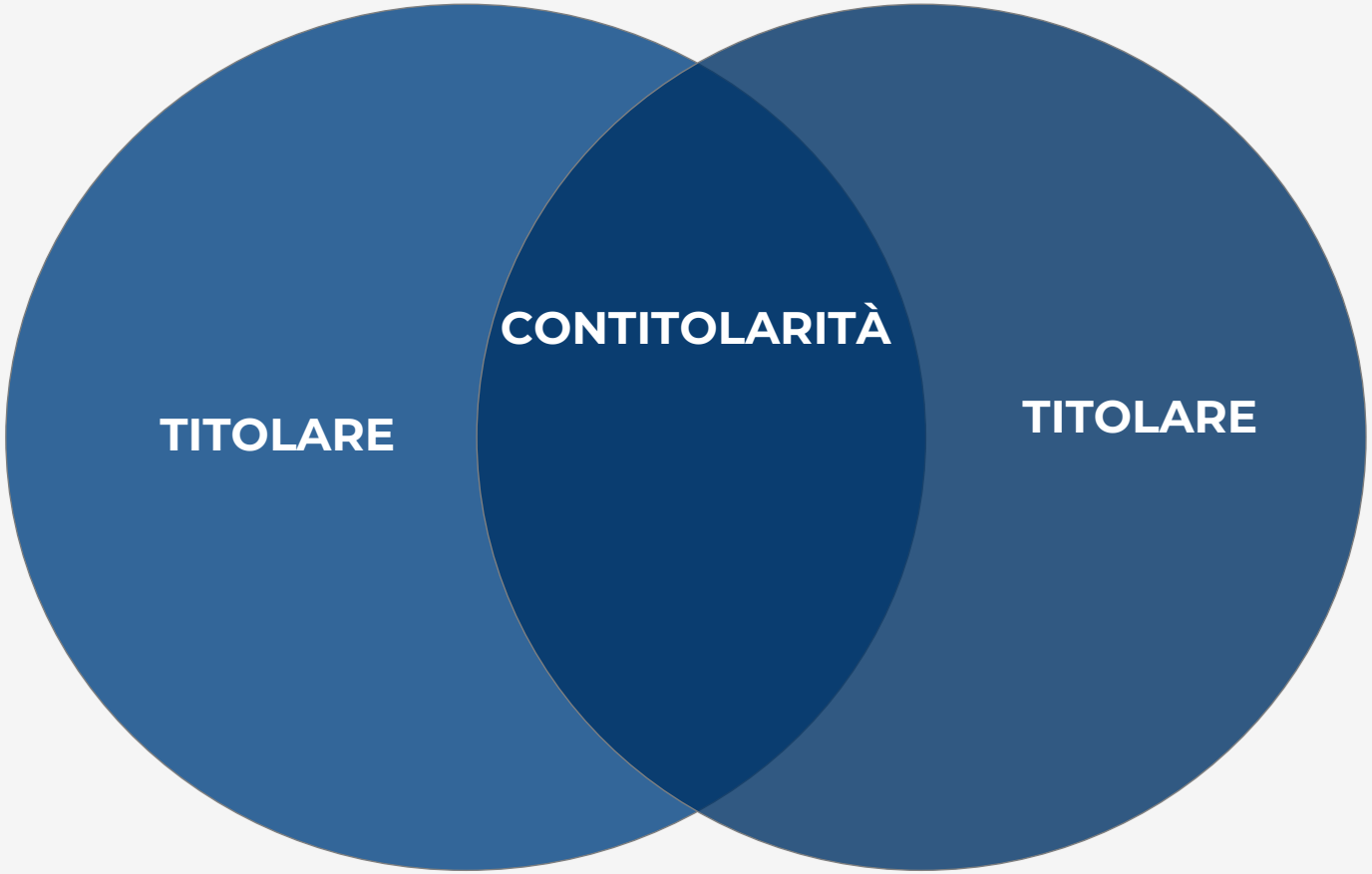
ESEMPI

Il Titolare è, dunque, **l'Ente nel suo complesso** ad esempio:

- l’impresa, a prescindere dalle sue dimensioni;
- l'ente pubblico;
- l’ente con o senza personalità giuridica;
- il libero professionista;
- le associazioni, le fondazioni e gli enti senza scopo di lucro.

CHI REDIGE E SOTTOSCRIVE GLI «ATTI PRIVACY» ALL'INTERNO DI UNA SOCIETÀ?

LA CONTITOLARITÀ DEL TRATTAMENTO



LA CONTITOLARITÀ DEL TRATTAMENTO

Art. 26 GDPR

Allorché due o più titolari del trattamento determinano ***congiuntamente le finalità e i mezzi*** *del trattamento, essi sono contitolari del trattamento.*

ESEMPIO

Si pensi a due imprese che producono **beni tra loro complementari** e che danno vita ad **un'iniziativa comune di marketing** o di promozione col fine di sollecitare o intercettare in modo coordinato i potenziali clienti.

DIVERSE TIPOLOGIE DI CONTITOLARITÀ

Secondo il Parere n. 1 del 2010 del WP29, è possibile configurare la contitolarità in due diversi tipi di situazioni:

a) quando una pluralità di soggetti condivide **tutte le finalità e i mezzi**;

b) quando una pluralità di soggetti condivide solo **alcune delle finalità o dei mezzi**: la condivisione dei mezzi e dei fini, infatti, può essere anche parziale.

Attenzione!

Il mero fatto che diversi soggetti cooperino all'elaborazione di dati personali, ad esempio **a catena**, non significa necessariamente che siano sempre corresponsabili!

Se mancano la condivisione di finalità o strumenti, in un insieme di operazioni comuni, **vi è un mero trasferimento** di dati fra due distinti titolari /responsabili del trattamento.

L'ACCORDO DI CONTITOLARITÀ: IL CONTENUTO

L’accordo in questione, deve indicare:

- l’**identità** dei Titolari;
- il **motivo** della sussistenza della contitolarità in ragione dei mezzi e delle finalità del trattamento;
- la distribuzione delle **responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR**;
- Le **misure di sicurezza** adottate;
- Gli adempimenti in caso di ***data breach*** *(*violazione che possa comportare, la distruzione, la perdita, la modifica, la divulgazione o l’accesso non autorizzati ai dati personali), prevedendo che ciascuna parte provveda prontamente a informare gli altri Titolari;
- **L’eventuale valutazione di impatto** che i contitolari si impegnano a fare;
- le rispettive funzioni di comunicazione delle **informazioni di cui agli articoli 13 e 14 GDPR**;
- nonché le **modalità di esercizio dei diritti** degli interessati dal momento che l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare.

L'ACCORDO DI CONTITOLARITÀ: LA CONOSCIBILITÀ

Art. 26 GDPR
Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato

L'informazione circa il rapporto di contitolarità è un ***adempimento imprescindibile*** *che consente di soddisfare l'ulteriore esigenza imposta dall'art. 26 del GDPR relativamente all'esercizio dei diritti da parte degli interessati.*

Fondazione Marco Biagi

UNIMORE

L'ACCORDO DI CONTITOLARITÀ: LA CONOSCIBILITÀ

CON QUALI MODALITÀ DEVE ESSERE RESO NOTO L'ACCORDO DI CONTITOLARITÀ?

Due tesi:

- È sufficiente l'**indicazione** del rapporto **nell'informativa** che viene consegnata all'interessato;
- Deve essere reso pubblico, ad esempio tramite la **pubblicazione** dello stesso **sul sito Internet**.

Possibile soluzione: pubblicazione di una «sintesi» dell'accordo.

SANZIONI

La violazione di una delle prescrizioni dell'Art. 26 (stipula, contenuto, conoscibilità dell'accordo di contitolarità) comporta una sanzione amministrativa pecuniaria fino a 10.000.000 di euro e, per le imprese, fino al 2% del fatturato mondiale totale annuo se superiore (**Art. 83, par. 4, lett. a GDPR**).

LA RESPONSABILITÀ DEI CONTITOLARI

L'**Art. 82, par. 4**, stabilisce che, in caso di titolarità congiunta, qualora il danno arrecato al trattamento sia imputabile a tutti i Titolari, ciascuno sarà reso responsabile **in solido** per l'intero ammontare del danno, salvo il **diritto di agire in regresso** nei confronti degli altri Titolari.

È POSSIBILE ACCERTARE LA «NON CONTITOLARITÀ»?

ESEMPIO:

Le Società Alfa e Beta hanno sede nel medesimo stabile.

Per accedere alla società Beta occorre necessariamente attraversare una zona videosorvegliata dalle telecamere della società Alfa.

A tali immagini videoregistrate accede, tuttavia, soltanto la società Alfa.

Beta che non condivide alcuna finalità del trattamento effettuato della società Alfa, né ne condivide i mezzi, è interessata a chiarire la sua estraneità a tale tipo di trattamento.

Lo può fare? In che modo?

I COMPITI DEL TITOLARE DEL TRATTAMENTO: LA “NOMINA” DEI SOGGETTI “GERARCHICAMENTE” SOTTOPOSTI

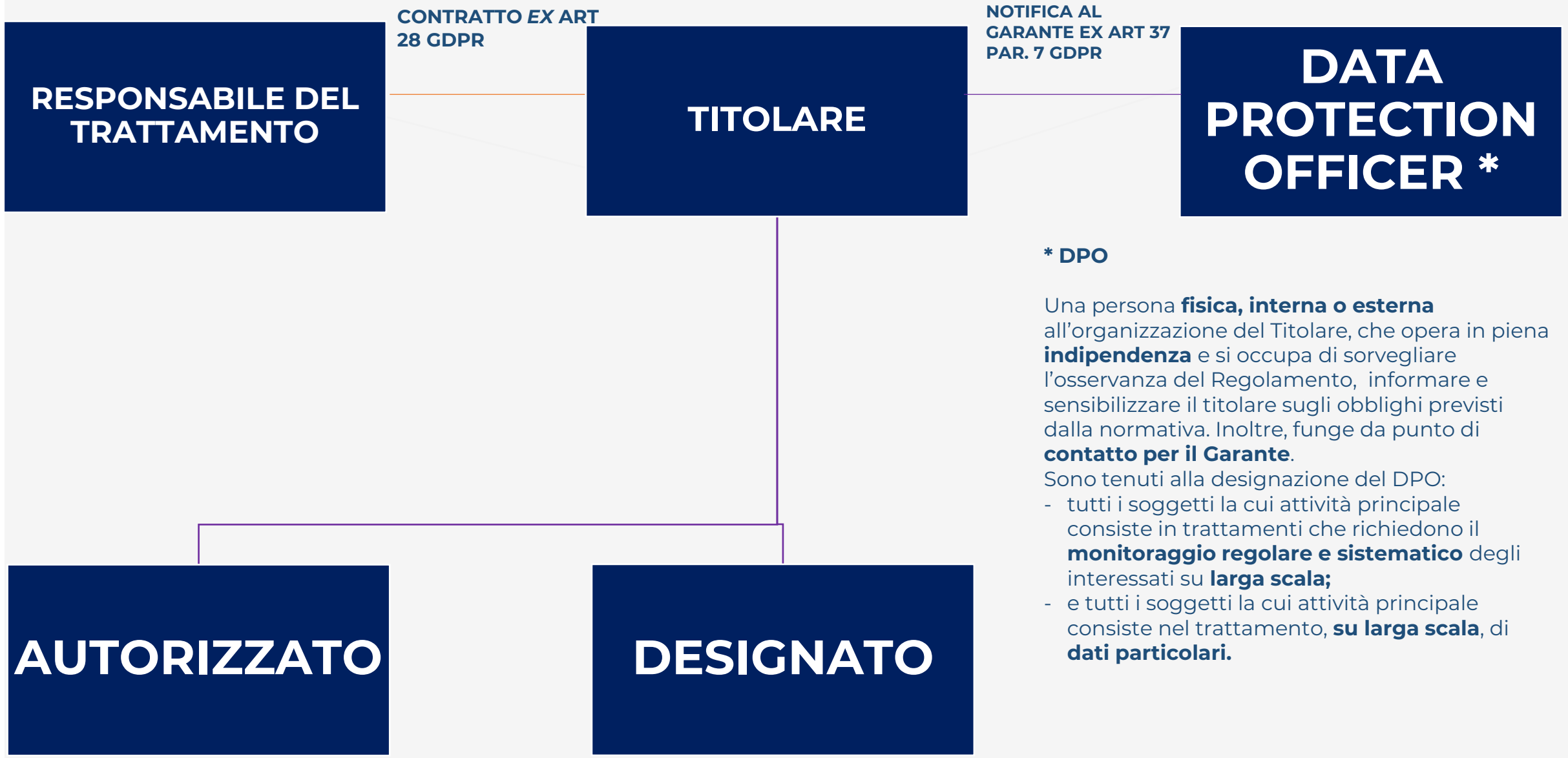
DESIGNATO AL TRATTAMENTO:

quella persona fisica che all’interno dell’organigramma aziendale, **coordina** il trattamento, ovvero riceve reclami, riceve segnalazioni, violazioni.

AUTORIZZATO AL TRATTAMENTO

(ex incaricato): quella persona fisica che, nell’ambito dell’attività di impresa, è legata al Titolare da un rapporto di **lavoro subordinato**, ma anche di collaborazione e che tratta dati personali per conto del Titolare.

ORGANIGRAMMA PRIVACY



*** DPO**

Una persona **fisica, interna o esterna** all'organizzazione del Titolare, che opera in piena **indipendenza** e si occupa di sorvegliare l'osservanza del Regolamento, informare e sensibilizzare il titolare sugli obblighi previsti dalla normativa. Inoltre, funge da punto di **contatto per il Garante**.

Sono tenuti alla designazione del DPO:

- tutti i soggetti la cui attività principale consiste in trattamenti che richiedono il **monitoraggio regolare e sistematico** degli interessati su **larga scala;**
- e tutti i soggetti la cui attività principale consiste nel trattamento, **su larga scala**, di **dati particolari.**

GLI AUTORIZZATI AL TRATTAMENTO

L'autorizzazione al trattamento è **necessaria** per giustificare i flussi di informazioni interni all'ente

MA

In un'ottica di semplificazione, il Garante ha specificato che chi prima del GDPR ha provveduto alla nomina degli **incaricati del trattamento** all'interno dell'azienda non è tenuto a convertirla.

INOLTRE

Per le **sole PMI**, il Garante ha ammesso che, la designazione possa avvenire attraverso un procedimento **SEMPLIFICATO** (che evita l'elaborazione di singoli atti circostanziati relativi distintamente a ciascun autorizzato). Purché risulti che **a)** Il lavoratore **sia assegnato stabilmente a una determinata unità; b)** siano individuati gli ambiti di **competenza** (in ordine ai trattamenti di dati consentiti) di quella unità mediante una previsione scritta (ad es. **nell´organigramma, nel contratto, nei mansionari,** ecc.).

Attenzione!

Tendenzialmente l'autorizzato al trattamento è un soggetto **interno** all'organizzazione ma ci possono essere ipotesi (rare) in cui il titolare instaura con un **soggetto esterno** un rapporto di collaborazione occasionale e non continuativo (es. manutentore esterno a chiamata), anche in questi casi è possibile prevedere un **atto di autorizzazione**.

UN CASO INTERESSANTE. LA CORRETTA QUALIFICAZIONE DELL'ORGANISMO DI VIGILANZA: AUTONOMO TITOLARE O RESPONSABILE DEL TRATTAMENTO?

Il Garante per la Protezione dei Dati Personali con il recente parere – nota prot. 17347 del 12.05.2020 – ha posto fine all'annoso dilemma:

l'ODV NON È

- **TITOLARE AUTONOMO**

Considerato che i compiti di iniziativa e controllo non sono determinati dall'organismo stesso, bensì dalla **legge e dall'organo dirigente** che nel modello di organizzazione e gestione definisce ad esempio l'attribuzione delle risorse, i mezzi e le misure di sicurezza.

- **Né RESPONSABILE DEL TRATTAMENTO**

l'OdV non è distinto dall'ente, ma è parte dello stesso.

QUINDI È AUTORIZZATO AL TRATTAMENTO

L'ente, titolare del trattamento, designerà i singoli membri dell'OdV quali soggetti autorizzati.

I COMPITI DEL TITOLARE DEL TRATTAMENTO: LA “NOMINA” DEL RESPONSABILE

Fra i compiti del Titolare del trattamento vi è quello di **individuare e designare** gli eventuali **responsabili** del trattamento.

CHI È IL RESPONSABILE DEL TRATTAMENTO?

Prima del GDPR, per la disciplina interna il responsabile era il **“preposto”** dal titolare al trattamento dei dati, ovvero colui che all’interno o all’esterno dell’organizzazione del titolare, gestiva il trattamento o una porzione di esso per conto del titolare che lo aveva designato.

Inoltre, ai sensi dell’articolo 29 del Codice Privacy, la designazione del responsabile non **era** obbligatoria ma **facoltativa.**

La prassi nazionale prevedeva due figure: **il responsabile interno ed il responsabile esterno.**

IL RESPONSABILE DEL TRATTAMENTO (data processor)

Con la riforma introdotta nell'ordinamento europeo dal nuovo Reg.(UE) n. 679/2016 il legislatore europeo, ha introdotto una diversa definizione di

"**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.**

IL RESPONSABILE DEL TRATTAMENTO (data processor)

La nuova definizione di “responsabile” ha aperto un **dibattito in dottrina** che ha visto opporsi due schieramenti:

- Alcuni sostengono che la figura del responsabile “interno” sia ancora pienamente ammissibile (tesi minoritaria);

- **Altri, al contrario, ritengono sia data soppressa** (tesi maggioritaria). La figura del “responsabile del trattamento” di cui all’art. 28 GDPR sarebbe ora riferibile, solamente ai soggetti “**esterni**” all’organizzazione del titolare, mentre per quelli “**interni**” troverebbero applicazione le norme relative ai soggetti **designati e autorizzati**, che operano sotto l’autorità del titolare.

ESEMPI

L'impresa Delta stipula un contratto con una società Gamma addetta all'elaborazione delle buste paga.

L'impresa Delta fornisce tutti i dati per le buste paga e i pagamenti. La società Gamma fornisce il sistema informatico e conserva i dati dei dipendenti dell'impresa Delta.

L'impresa Delta è il titolare del trattamento e la società Gamma, addetta all'elaborazione delle buste paga, è il responsabile del trattamento.

Ancora, a titolo esemplificativo si pensi:

- al servizio svolto dalle società di consulenza **tecnica**, **fiscale e amministrativa**;
- alle **associazioni di categoria** che offrono servizi agli associati a cui le PMI aderiscono;
- all'**RSPP** ovvero al responsabile del servizio di protezione e prevenzione.

ORGANIGRAMMA PRIVACY

RESPONSABILE DEL TRATTAMENTO

CONTRATTO *EX* ART 28 GDPR

TITOLARE

NOTIFICA AL GARANTE EX ART 37 PAR. 7 GDPR

DATA PROTECTION OFFICER *

AUTORIZZATO

DESIGNATO

*** DPO**

Una persona **fisica, interna o esterna** all'organizzazione del Titolare, che opera in piena **indipendenza** e si occupa di sorvegliare l'osservanza del Regolamento, informare e sensibilizzare il titolare sugli obblighi previsti dalla normativa. Inoltre, funge da punto di **contatto per il Garante**.

Sono tenuti alla designazione del DPO:

- tutti i soggetti la cui attività principale consiste in trattamenti che richiedono il **monitoraggio regolare e sistematico** degli interessati su **larga scala;**
- e tutti i soggetti la cui attività principale consiste nel trattamento, **su larga scala**, di **dati particolari.**

LA SCELTA DEL RESPONSABILE

Secondo il Regolamento, il Titolare può servirsi solo di quei soggetti, siano essi persone fisiche o giuridiche, **“responsabili”,** cioè capaci di garantire che l’attività di **trattamento** sia **conforme** alla **normativa** e in grado di **proteggere** i **diritti degli interessati**.

Cosa significa?

LA SCELTA DEL RESPONSABILE

Il Responsabile deve essere in grado di **presentare garanzie sufficienti** in termini di:

A) conoscenza specialistica (es. competenze tecniche in materia di misure di sicurezza e violazioni dei dati);

A) affidabilità;

B) Risorse per mettere in atto le misure tecniche e organizzative necessarie (Considerando 81 GDPR).

Compito specifico del titolare è: **valutare il rischio** del trattamento che pone in essere tramite i responsabili.

Il titolare deve verificare che il responsabile **agisca secondo le modalità imposte dalla normativa** (deve verificare le **misure di sicurezza attuate**; l'eventuale **nomina del DPO** e lo svolgimento di una **valutazione di impatto** se necessaria).

Suggerimento: potrebbe essere una buona prassi inviare un questionario periodico (semestrale o annuale) in cui si chiede al responsabile di rendicontare gli adempimenti privacy.

CONTRATTO TRA TITOLARE E RESPONSABILE

Ai fini della validità del rapporto tra Titolare e responsabile del trattamento, è necessario siglare un contratto o un qualsiasi atto giuridico che abbia forma scritta (**data protection agreement**), come previsto dall'articolo 28 del GDPR.

Cosa deve prevedere?

CONTRATTO TRA TITOLARE E RESPONSABILE

1- Obblighi generali del Responsabile del trattamento

Il Responsabile provvede a:

a) individuare le persone fisiche autorizzate al trattamento (è infatti tenuto a **garantire la riservatezza dei dati**);

b) Redigere ed aggiornare il **registro dei trattamenti.**

2– Obblighi del Responsabile relativi alle misure di sicurezza

Il Responsabile è tenuto ad osservare gli obblighi in relazione alle misure di sicurezza previste dalla normativa vigente.

Nel contratto possono essere indicate, ad esempio, le **misure di sicurezza minime; inoltre** può essere previsto che il Responsabile metta in atto **le procedure per testare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** per la sicurezza del trattamento).

Fondazione Marco Biagi

UNIMORE

CONTRATTO TRA TITOLARE E RESPONSABILE

3 – Obblighi del Responsabile del trattamento in caso di violazione dei dati

Deve essere previsto che il Responsabile del trattamento informi il Titolare del trattamento, **tempestivamente** di qualsiasi violazione di dati personali.

Un suggerimento può essere quello di individuare un termine specifico, ad esempio 24 ore, per permettere al titolare di notificare al Garante la violazione entro il termine di 72 ore dalla scoperta della violazione stessa.

4 – Subresponsabili

(soggetti che assumono il ruolo di responsabili nei confronti di un altro responsabile)

Gli eventuali Subresponsabili devono essere selezionati tra soggetti che **per esperienza, capacità e affidabilità** forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate.

•Inoltre il responsabile dovrà ottenere:

a) Autorizzazione preventiva dal Titolare;

b)Predisposizione degli **strumenti** utili ad un **controllo effettivo** sull'attività del sub-responsabile;

c)Redazione di un **accordo di ripartizioni** circa gli oneri e le responsabilità.

Il responsabile risponde dinanzi al titolare dell'inadempimento del sub-responsabile.

CONTRATTO TRA TITOLARE E RESPONSABILE

5 – Controlli

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal contratto e consente e contribuisce “alle attività di revisione, comprese le **ispezioni**, realizzate dal titolare del trattamento”.

6 – Trasferimento dei dati

Buona prassi è quella di prevedere un **divieto generale di trasferimento** dei dati personali oggetto di trattamento **verso un Paese terzo** o un’organizzazione internazionale.
Prevedendo che - nelle ipotesi in cui per eseguire le operazioni di trattamento, il Responsabile non possa evitare di trasferire dati verso un Paese terzo o un’organizzazione internazionale - dovrà farsi preventivamente ed esplicitamente **autorizzare dal Titolare** del trattamento, indirizzando a quest’ultimo una richiesta scritta e motivata.

Questo perché i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento prevede.

CONTRATTO TRA TITOLARE E RESPONSABILE

Il contratto o altro atto giuridico **può basarsi**, in tutto o in parte, su **clausole contrattuali tipo** nell'ipotesi in cui non sia sottoscritto uno specifico contratto tra le parti, una sorta di contratto standard che dovrà essere personalizzato dalle parti contrattuali.

In proposito la **Commissione europea ha adottato la Decisione di esecuzione (UE) 2021/915** relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679.

Suggerimento

Il contratto può essere a titolo oneroso o gratuito, se è a titolo gratuito è bene specificare nel contratto stesso che la nomina non comporta alcun diritto ad uno compenso ulteriore rispetto a quanto eventualmente pattuito per il servizio fornito.

I COMPITI DEL RESPONSABILE

- istituire un **registro dei trattamenti** per conto di ciascun titolare (art. 30, par.2 del GDPR);
- informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza **della violazione dei dati**(art. 33, par. 2);
- designare un responsabile della protezione dei dati **DPO** ogniqualvolta sia necessario (art. 37);
- adottare **misure tecniche e organizzative** adeguate al rischio. Sulle misure tecniche e organizzative il responsabile ha una certa **autonomia,** purché garantiscano un livello di sicurezza adeguato al rischio (art 32);
- nominare un **rappresentante**, qualora non sia stabilito nel territorio europeo (art. 27, par.1 del GDPR);
- **cooperare** con le autorità di controllo (art. 31 del GDPR)

E SE IL TITOLARE È ANCHE RESPONSABILE?

Ci si riferisce alle ipotesi in cui l'azienda rivesta sia il ruolo di Titolare nell'ambito della propria attività di impresa, sia quello di responsabile del trattamento in virtù dell'attività svolta per conto di un altro Titolare del trattamento, (es. modello **"Business-to-Business"**).

LE VIOLAZIONI DEL RESPONSABILE

Il responsabile del trattamento può rispondere nel caso di violazione:

a) di un obbligo previsto dal GDPR;

b) di un **obbligo contrattuale** derivante dal contratto con il titolare.

Tra le obbligazioni condivise con il titolare, rientrano: l'adozione delle idonee **misure di sicurezza**, la cooperazione con il titolare per le valutazione d'impatto (**DPIA**) e/o in caso di ***data breach*.**

La sanzione amministrativa pecuniaria ammonta fino a euro **10.000.000,00 o per le imprese fino al 2%** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par.4 GDPR).

Fondazione Marco Biagi

UNIMORE

LE VIOLAZIONI DEL RESPONSABILE

• Rapporti con l'interessato:
Tra titolare e responsabile **vi è un vincolo risarcitorio solidale.**

• Rapporti interni (art 82 par. 5 GDPR)

Se verso l'interessato vale il principio della solidarietà, nei rapporti interni vale la **quota di responsabilità** il cui **grado** dovrà essere valutato in base ad alcune circostanze quali ad esempio la presenza di clausole contrattuali di **manleva**, l'aver impartito o meno **istruzioni specifiche o generiche** al responsabile.

Attenzione alle clausole limitative della responsabilità!

Lo **squilibrio** contrattuale tra titolare e responsabile non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati!

IL CONSULENTE DEL LAVORO

Nel 2018 il Consiglio nazionale dei consulenti del lavoro ha sottoposto al Garante un quesito relativo alle corretta qualificazioni del consulente del lavoro:

Il garante ha risposto distinguendo il segmento di attività:

a)Se il consulente del lavoro tratta i dati dei **propri dipendenti o clienti è titolare del trattamento.**

E la **base giuridica** che facoltizza il trattamento in capo al soggetto in questione è rinvenibile **nell'esecuzione del contratto** (art. 6, par. 1, lett. b, del Regolamento).

b) Se il consulente tratta i dati dei dipendenti del cliente occorre fare riferimento alla figura **del responsabile**.

In questo caso la **base normativa** che legittima il trattamento dei dati personali, va individuata in capo al suo cliente (ovverosia il datore di lavoro/titolare) ai sensi dell'art. 9, par. 2, lett. b), del Regolamento: infatti, la legittimità del trattamento si **"trasferisce"** alle operazioni svolte dal consulente del lavoro in ragione del contratto di sua designazione a responsabile del trattamento.

IL MEDICO COMPETENTE

Lo stesso interrogativo circa l'esatta qualifica ha riguardato il medico competente.

La funzione di medico competente è espressione di un **interesse pubblico** (tutela del lavoratore e della collettività), individuato e disciplinato dalla **legge** e, in quanto tale, sottratta alla sfera di competenza del datore di lavoro e ai relativi poteri.

In tale quadro, quindi, il medico non tratta i dati per conto del datore di lavoro ma, in qualità di **titolare del trattamento** (artt. 4, n. 7 e 24 del Regolamento), in base a specifiche diposizioni di legge finalizzate anzitutto al perseguimento dell'interesse pubblico di tutela della salute nei luoghi di lavoro e della collettività.

SANZIONE DEL GARANTE PRIVACY ALLA REGIONE LAZIO NON AVEVA DESIGNATO RESPONSABILE DEL TRATTAMENTO LA COOPERATIVA CHE GESTIVA IL CALL CENTER DEL CUP

Il Garante per la protezione dei dati personali ha **sanzionato la Regione Lazio per 75.000 euro** per non aver nominato responsabile del trattamento dati la Società cooperativa che gestiva le prenotazioni delle prestazioni sanitarie.

Il Garante ha **invece ammonito** la Società cooperativa perché aveva più volte rappresentato alla Regione la necessità di essere nominata responsabile del trattamento e messo in atto misure conformi alla disciplina privacy, istituendo, ad esempio, il registro dei trattamenti.

INOLTRE

Il Garante ha evidenziato che in assenza di **un contratto o di altro atto giuridico,** stipulato per **iscritto** tra titolare e responsabile **manca la di base giuridica** su cui ogni trattamento deve fondarsi.