Figure soggettive

Giovanni Maria Riccio
gmriccio@unisa.it

Di cosa parliamo oggi?

- Titolare del trattamento
- Responsabile del trattamento
- Contitolari del trattamento
- Rappresentanti di titolari
- Subresponsabile
- Obblighi e responsabilità
- Registri del trattamento

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
- Analisi fattuale, non formalistica: es. indicazione di un soggetto quale titolare in un contratto

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

Problema di traduzione

- Titolare (art. 4, lett. f, Codice privacy = Responsabile)
- Responsabile (art. 4, lett. g, Codice privacy = Incaricato)
- Nessun problema nel GDPR

Titolare - Persone giuridiche

- Provv. 9 dicembre 1997 (Individuazione del titolare del trattamento) – Doc. Web n. 30915
- **Ferrovie dello Stato S.p.A.**
- Qualora il trattamento sia effettuato da una persona giuridica, da una pubblica amministrazione o da altro organismo, il "titolare" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.) e non una delle persone fisiche che operano nella struttura. Questi, al più, possono essere qualificati come "responsabile"

Titolare – Appalti di servizi

- **GPDP 29 aprile 2009**
  Servizi postali: Poste Italiane Doc. Web n. 1617709
- La società appaltatrice per i servizi di recapito della corrispondenza è responsabile o titolare?
- *"l'esternalizzazione da parte della società di compiti connessi all'espletamento del servizio postale (e dei connessi trattamenti finalizzati al recapito della corrispondenza)"* può costituire una soluzione organizzativa pienamente legittima *"a condizione che le società appaltatrici […] siano individuate secondo i criteri ex art. 29, comma 2 del Codice Privacy"*

GPDP 12 maggio 2011
Servizi bancari

- **Doc. Web n. 1813953**
- le società esterne alle banche che gestiscono in *outsourcing* i sistemi informativi contenenti i dati della clientela, sono considerati responsabili del trattamento e non titolari
- È rimesso alle banche il potere di assumere decisioni relative alle finalità del trattamento; impartire istruzioni e direttive vincolanti nei confronti delle società di gestione dei sistemi informativi; svolgere funzioni di controllo rispetto all'operato delle medesime e degli incaricati delle stesse

GPDP 4 luglio 2011
Servizi di telefonia

- **Doc. Web n. 1821257**
- Gli *outsourcer* sono qualificati come responsabili esterni difettando i presupposti per il riconoscimento di una loro autonoma titolarità. Infatti, *ex* artt. 4, comma 1, lett. f) e 28 del Codice Privacy, il titolare è il soggetto *"cui competono […] le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati"* e che esercita *"un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza".*

GPDP 15 settembre 2011
Buongiorno – Servizi VAS

- **Doc Web. n. 1849872**
- Da un ciclo di accertamenti ispettivi sulle campagne di marketing in materia di protezione dei dati personali, l'attenzione del Garante si è soffermata sulla Buongiorno S.p.a., una società che eroga in prevalenza servizi VAS (servizi di valore aggiunto), cioè suonerie, contenuti digitalizzati, editoria ecc.
- Secondo il Garante, non è ipotizzabile che la Buongiorno S.p.a. ricopra, a seconda dell'operatore di telefonia mobile al quale l'utente risulta abbonato, talvolta il ruolo di titolare e tal'altra quello di responsabile. Secondo l'Autorità, la società è la titolare del trattamento per la parte di propria competenza a prescindere dall'operatore a cui l'utente è abbonato.

Legittimazione processuale

- La natura di titolare del trattamento incide anche sotto il profilo della legittimazione processuale
- Il provvedimento con il quale il Garante per la protezione dei dati personali prescrive, ai sensi degli artt. 143, comma 1, lett. b), e 154, comma 1, lett. c), del d.lgs. n. 196 del 2003 (cd. codice della "privacy"), l'adozione delle necessarie misure, anche di carattere tecnico, per le cd. chiamate "mute", non integra una sanzione amministrativa, sicché il soggetto legittimato all'opposizione, in sé diretta a sottoporre a controllo giurisdizionale la situazione soggettiva su cui il provvedimento ha inciso, non è qualunque titolare del trattamento dei dati personali ma lo specifico titolare destinatario della prescrizione (nella specie, Enel Energia s.p.a., e non anche la società proprietaria della piattaforma informatica messa a disposizione della prima)
- **Cass. civ. Sez. I, 04/02/2016, n. 2196**

Contitolarità del trattamento

- Quando "*determinano congiuntamente le finalità e i mezzi del trattamento*"
- determinano in modo trasparente, mediante un **accordo interno**, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento
- Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato
- L'interessato può esercitare i **propri diritti** nei confronti di e contro ciascun titolare del trattamento

Titolarità comune e contitolarità

- U.K. Information Commissioner's Office: Key definitions of the Data Protection Act
- **Contitolari** determinano insieme le finalità e le modalità del trattamento
- **Titolari in comune** condividono dati personali, ma ognuno elabora autonomamente le modalità di trattamento

Esempio

- Un'agenzia invia dati personali dei suoi clienti alle compagnie aeree e a una catena d'alberghi per effettuare delle prenotazioni per un pacchetto viaggi. La compagnia aerea e l'albergo confermano la disponibilità dei posti e delle camere richiesti. L'agenzia emette i documenti di viaggio e i voucher per i suoi clienti.
- **Chi è titolare del trattamento?**

Esempio n. 2

- L'agenzia, la catena alberghiera e la compagnia aerea decidono di creare una piattaforma comune su Internet per migliorare la loro cooperazione nella gestione delle prenotazioni. Concordano insieme aspetti importanti degli strumenti da utilizzare, ad es. quali dati saranno conservati, come saranno distribuite e confermate le prenotazioni, e chi potrà avere accesso alle informazioni conservate. Decidono inoltre di condividere i dati dei loro clienti per svolgere azioni integrate di marketing.
- **Chi è titolare del trattamento?**

Esempio n. 3

- Centri di raccolta di dati medici
- Es. Registro dei tumori o simili registri
- **Chi è il titolare del trattamento?**
- Esigenze di tutelare i soggetti interessati e consentire l'esercizio dei diritti

Responsabile del trattamento

- Chi può essere responsabile del trattamento?
- Soggetti che presentino garanzie sufficienti per **mettere in atto** misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato
- Valutazione che deve essere condotta dal **titolare del trattamento**

Per conto del titolare

- Significa che il responsabilità del trattamento agisce per finalità non proprie, ma determinate dal titolare
- Ad esempio, la società Alfa incarica la società Beta di compiere una campagna marketing e le comunica il suo DB proprietario
- Se la società Beta utilizza il medesimo DB per un altro cliente, non sta agendo in qualità di responsabile del trattamento di Alfa

NOMINA A RESPONSABILE DEL TRATTAMENTO

ai sensi dell'art. 29 del D.lgs. 196/2003

Alfa S.r.l., con sede legale in Via _____, Roma, iscritta al Registro delle imprese di Roma al n° _____ (di seguito per brevità anche il "**Titolare**" o la **"Alfa"**)

e

Beta Ltd., con sede legale Londra (Regno Unito), _____, company registration number: _____ (di seguito per brevità anche o il **"Responsabile"**)

di seguito **"Parte"** e collettivamente **"Parti"**

Atto di nomina

- Per iscritto: sono disciplinati da un contratto o da altro atto giuridico
- Onere della prova
- Il contratto (o altro atto) deve prevedere:

ü la materia disciplinata
ü la durata del trattamento
ü la natura e la finalità del trattamento
ü il tipo di dati personali
ü le categorie di interessati
ü gli obblighi e i diritti del titolare del trattamento

Atto di nomina

Cosa deve contenere, tra l'altro, che il responsabile:

a) Tratti i dati su istruzione documentata del titolare del trattamento

b) Garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza

c) Adotti le misure di sicurezza

d) Cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti

Clausole facoltative

- Diritto al rimborso delle eventuali spese sostenute per attenersi alla istruzioni del titolare
- Responsabilità del responsabile per le azioni dei suoi incaricati del trattamento
- Obbligo di notifica al titolare per trattamenti fuori da UE
- Obbligo di progettare ogni nuovo trattamento con Privacy by Design e Privacy by Default (v.)
- Possibilità di audit (v.)
- Manleve e cooperazione (v.)

Clausole contrattuali tipo

- Art. 28, par. 7, 8, 9
- Commissione o Garante potrebbero dettare delle clausole contrattuali tipo per la nomina del responsabile del trattamento

Rappresentanti di titolari

- Nel caso di soggetti extra UE che

ü Offrono beni o servizi a cittadini UE

ü Monitorano cittadini UE

Obbligatoria la nomina di un 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”

Rappresentanti di titolari

Il rappresentante è stabilito in uno degli Stati membri in cui si trovano gli interessati – Scelta oculata della giurisdizione "migliore"

- Designazione scritta (Cons. 80)
- Può essere un soggetto esterno alla società?
- Qual è la differenza con il DPO, se sono entrambi punti di contatto?

Non è necessario:

- trattamenti occasionali
- non include il trattamento, su larga scala, di dati sensibili o giudiziari

Subresponsabile

- Sinora il Garante aveva sempre escluso la possibilità di nominare un subresponsabile, ossia un responsabile nominato da un responsabile
- Contratti di appalto: nomina di subresponsabili per i subappaltatori

Presupporti per la nomina del subresponsabile

- Autorizzazione del titolare
- Scritta
- Specifica o generale
- Eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento
- Il subresponsabile deve quindi essere indicato

Clausole standard

- Contratti identici a quelli sottoscritti dai responsabili
- Due diligence iniziale sul sub-responsabile
- Possibilità di audit/controllo sul sub-responsabile
- Revoca del consenso al sub-responsabile
- Responsabilità del responsabile per l'attività del sub-responsabile nei confronti del titolare

Obblighi del titolare del trattamento

- Rispettare il GDPR / accountability
- Adottare misure tecniche e organizzative
- Adottare il Registro dei trattamenti
- Cooperare con l'Autorità Garante
- Notifica in caso di data breach
- Nomina del DPO

Accountability

- Art. 6(2) Direttiva: obbligo di assicurare la compliance con i principi della direttiva
- Art. 5(2) GDPR + Cons. 85: obbligo di assicurare e **di dimostrare** la compliance con i principi del GDPR

Accountability

- Art. 25(1): *"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche"*
- *misure tecniche e organizzative adeguate*
- Dette misure sono riesaminate e aggiornate qualora necessario

Accountability

- Adesione a **codici di condotta** e **certificazioni**
- Quali? Valgono le certificazioni esistenti?
- Eliminano la responsabilità? La limitano?
- Sono strumenti utili?

Adottare misure tecniche e organizzative

- Art. 6(2) Direttiva: il titolare del trattamento deve garantire che le sue attività di trattamento siano conformi ai requisiti della direttiva.
- Art. 24 GDPR: il titolare è responsabile dell'implementazione di misure tecniche e organizzative appropriate per garantire e dimostrare che le sue attività di trattamento siano conformi ai requisiti del GDPR.

+ adeguate politiche sulla privacy

+ adesione ai codici di condotta e adozione di meccanismi di certificazione approvati può essere prova di conformità

Cooperare con l’Autorità Garante

- La direttiva non richiede esplicitamente ai titolari del trattamento di cooperare con l’Autorità Garante
- Art. 31 GDPR: Il titolare del trattamento, il responsabile del trattamento e, ove applicabile, il loro rappresentante cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

Data Breach

- Direttiva: nessun obbligo (legislazione nazionale)
- Art. 33 GDPR: obbligo del titolare, non DPO
- Max 72 ore
- Descrizione del breach, numero dei soggetti interessati, tipologie di dati
- Assessment sui rischi
- Misure per controbattere o mitigare

Responsabilità

- Centro di imputazione della responsabilità
- Civile e amministrativa
- Penale
- Sussiste un obbligo per il responsabile del trattamento di “avvisare” il titolare in caso di violazioni di legge?
- Clausole di esonero di responsabilità a favore del titolare

Art. 82

- Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento
- Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.
- Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento

Solidarietà

- Qualora più titolari o responsabili oppure entrambi il titolare e il responsabile siano coinvolti nello stesso trattamento e siano, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato
- Qualora un titolare o un abbia pagato l'intero risarcimento del danno, tale titolare o responsabile ha il diritto di reclamare dagli altri titolari o responsabili coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno

Sanzioni

- Sanzioni specifiche in caso di mancata nomina?
- Possibilità di adottare clausole di manleva nei rapporti interni?

Registri del trattamento

- Art. 30: Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità
- Sostituisce l'obbligo di notifica al Garante
- Tenuti in forma scritta o in formato elettronico
- A disposizione dell'Autorità in caso di controlli o ispezioni
- Stabilire modalità di conservazione del Registro

Informazioni nei Registri

- Nomi e dati di contatto di titolare, responsabile, contitolare e DPO
- Finalità del trattamento
- Descrizione delle categorie di interessati e delle categorie di dati personali (v. slide successiva)
- Categorie di destinatari a cui i dati personali sono stati o saranno comunicati
- Trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale
- Termini ultimi previsti per la cancellazione delle diverse categorie di dati
- Descrizione generale delle misure di sicurezza tecniche e organizzative

Finalità del trattamento

- Attività amministrative
- Fatturazione
- Gestione clientela
- Ricerca scientifica
- Marketing
- Profilazione
- Geolocalizzazione
- Ecc.

Tipologie di dati

- dati che rivelano l'origine razziale o etnica (art. 9)
- dati che rivelano le opinioni politiche (art. 9)
- dati che rivelano le convinzioni religiose o filosofiche (art. 9)
- dati che rivelano l'appartenenza sindacale (art. 9)
- dati genetici (artt. 4, par. 1, n. 13 e 9)
- dati biometrici (artt. 4, par . 1, n. 14 e 9)
- dati relativi alla salute (artt. 4, par. 1, n. 15 e 9)
- dati relativi alla vita/orientamento sessuale (art. 9)
- dati relativi a condanne penali e reati (art. 10)

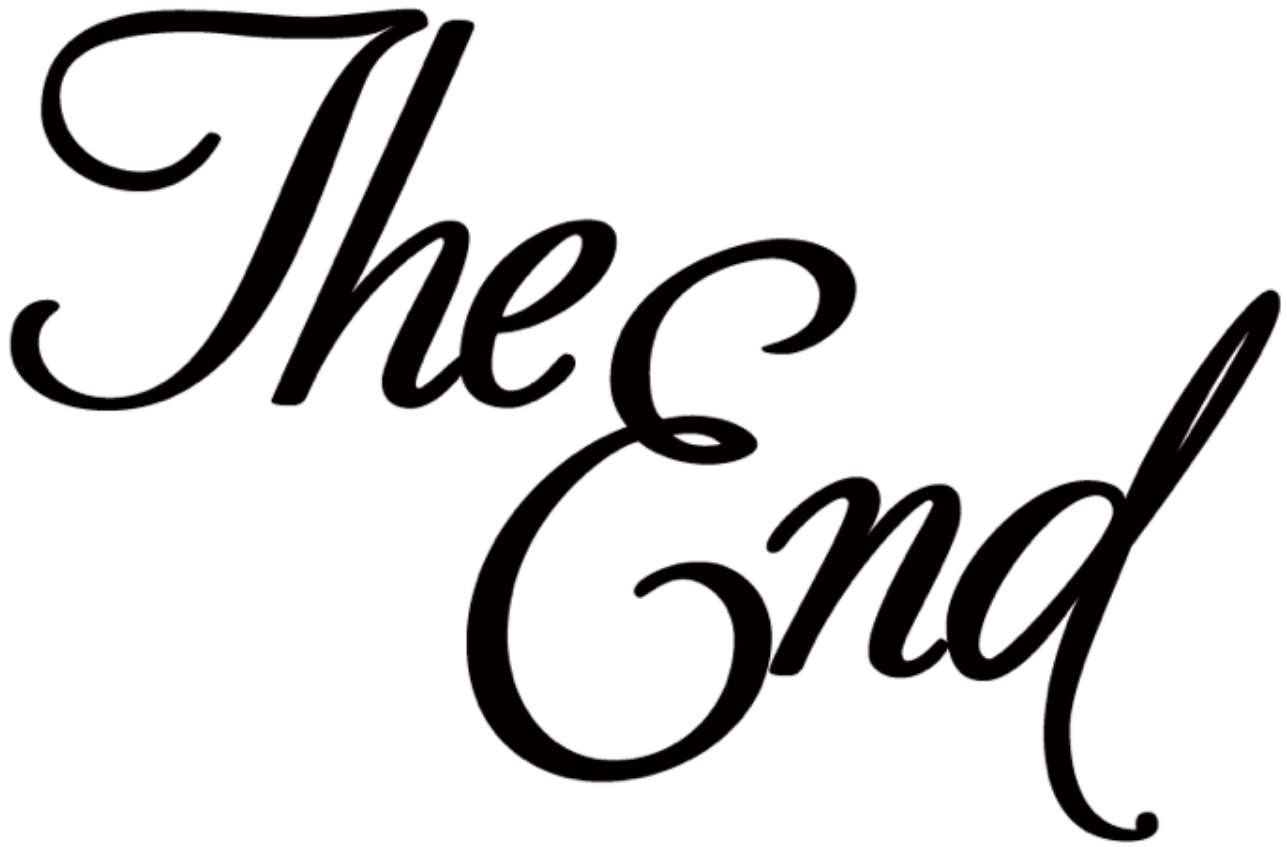
Registro del responsabile

- Nomi e dati di contatto di responsabile, di ogni titolare, del rappresentante del titolare e del DPO
- Categorie dei dati trattati per conto del titolare
- Trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale
- Descrizione generale delle misure di sicurezza tecniche e organizzative

Commission de la Protection de la Vie Privée - Belgio

Modèle de Registre des activités de traitement

La Commission vie privée met à disposition un modèle de Regi
responsables de traitements afin d'aider les entreprises et orga
Registre des activités de traitement.


The End