SOMMARIO

Prefazione **4**

1. L'Autorità nazionale di controllo: il Garante **5**

2. Gli "attori" principali del trattamento **11**
2.1 Titolare, Contitolari e Responsabile - alcune considerazioni 12
2.2 Rapporti tra i soggetti 23

3. Il trattamento dei dati **27**
3.1 Principi fondamentali 28
3.1.1 Liceità 29
3.1.2 Trasparenza (l'informativa) 33
3.1.3 Responsabilizzazione ("accountability") 44

4. I diritti degli interessati **47**
4.1 Il diritto di essere informato 48
4.2 I diritti degli interessati 49
4.2.1 Il diritto di accedere ai propri dati personali (art.15 del RGPD) 50
4.2.2 Il diritto alla rettifica e alla cancellazione (art.17 del RGPD) 51
4.2.3 Il diritto di limitazione (art.18 del RGPD) 51
4.2.4 Il diritto alla portabilità dei dati (art.20 del RGPD) 52
4.2.5 Il diritto di opposizione (art.21 del RGPD) 55
4.2.6 Il diritto a non essere sottoposto ad un processo decisionale automatizzato - compresa la profilazione (art.22 del RGPD). 55
4.3 - Limitazioni ai diritti (art.23 del RGPD) 56

5. Obblighi di titolari e responsabili **57**
5.1 Il Registro delle attività di trattamento 58
5.2 Il Responsabile della Protezione dei Dati - RPD/DPO (art.37 del RGPD) 59
5.3 La "Privacy by design e by default" - PbDD (art.25 RGPD) 71
5.4 La valutazione d'Impatto - acronimo in inglese DPIA (art 35 RGPD) 77
5.5 La "pseudonimizzazione" 87
5.6 La Notifica e la Comunicazione di violazioni 91

Allegati - tratti dalle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679 [WP250 rev.01], del 06.02.2018

Prefazione

Il Regolamento UE 2016/679, il Regolamento Generale sulla Protezione dei Dati personali (abbreviato con RGPD o GDPR, acronimo in inglese), è ormai una realtà con la quale tutti i soggetti pubblici e privati devono confrontarsi nella prassi quotidiana quando vogliono o devono trattare dati personali, per qualsiasi finalità e in qualsiasi contesto.

Il RGPD si inserisce in un quadro normativo già aperto dalla Direttiva comunitaria CE n.46 del 1995, recepita in Italia con la Legge 675/1996, evoluta poi nel D.Lgs. 196/2003 (il c.d. "Codice della privacy").

L'impianto normativo creato, al cui vertice si pone oggi il RGPD, conferma e rafforza il principio di base sancito dai legislatori europei: la protezione dei dati personali è un **diritto** fondamentale.

Oggi, il Regolamento, **responsabilizza** in maniera molto forte, e superiore rispetto al passato, i soggetti principali di ogni trattamento di dati personali; imponendo, al titolare e al responsabile, di pensare in anticipo le finalità e le modalità dei trattamenti e di costruirne correttamente - e in modo documentabile - l'impalcatura giuridica e organizzativa.

In questa nuova architettura anche le Autorità nazionali di controllo (come il Garante) trovano conferme e novità. Conferme, in quanto Autorità indipendenti e incaricate di garantire la reale attuazione delle norme in tutti gli Stati membri; novità, soprattutto in termini di una più stringente ed efficace cooperazione e di obblighi di assistenza reciproca, come per esempio il nuovo organismo creato dal RGPD, il **Comitato Europeo per la Protezione dei Dati** (CEPD, *European Data Protection Board - EDPB*). Il Comitato, che ha personalità giuridica e al quale sono demandate funzioni al tempo stesso di guida e di decisore ultimo nei casi controversi, è l'erede dell'ex "Gruppo Articolo 29" - WP29 (previsto dalla Direttiva del 1995 come organo consultivo della Commissione europea e degli interessati nazionali). Il Comitato si compone di un rappresentante per ciascuna Autorità nazionale di controllo (fra cui il Garante), della Commissione europea e del Garante Europeo per la Protezione dei Dati (GEPD, *European Data Protection Supervisor - EDPS*). Di fatto, è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le Autorità competenti per la protezione dei dati dell'UE . La Commissione europea e l'Autorità di vigilanza EFTA hanno titolo a partecipare alle attività e alle riunioni del Comitato senza diritto di voto.

Capitolo 1

L'Autorità nazionale di controllo: il Garante

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196), come modificato dal D.Lgs. 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51). Tale autorità ha sede, attualmente, in Piazza Venezia n.11 a Roma (RM).

I Compiti del Garante sono definiti dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il D.Lgs. 10 agosto 2018, n. 101, oltre che da vari altri atti normativi italiani e internazionali.

A titolo esemplificativo, ma non esaustivo, il Garante si occupa di:
- controllare che i trattamenti di dati personali siano conformi al Regolamento nonché a leggi e regolamenti nazionali e prescrivere, ove necessario, ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento nel rispetto dei diritti e delle libertà fondamentali degli individui;
- collaborare con le altre autorità di controllo e prestare assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del Regolamento;
- esaminare reclami;
- (nel caso di trattamenti che violano le disposizioni del Regolamento) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento e ingiungere di conformare i trattamenti alle disposizioni del Regolamento; imporre una limitazione provvisoria o definitiva del trattamento, incluso il divieto di trattamento; ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento;
- adottare i provvedimenti previsti dalla normativa in materia di protezione dei dati personali;
- segnalare, anche di propria iniziativa, al Parlamento e altri organismi e istituzioni l'esigenza di adottare atti normativi e amministrativi relativi alle questioni riguardanti la protezione dei dati personali;
- formulare pareri su proposte di atti normativi e amministrativi;
- partecipare alla discussione su iniziative normative con audizioni presso il Parlamento;
- predisporre una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla privacy da trasmettere al Parlamento e al Governo;
- partecipare alle attività dell'Unione europea ed internazionali di settore, anche in funzione di controllo e assistenza relativamente ai sistemi di informazione Europol, Schengen, VIS, e altri;
- curare l'informazione e sviluppare la consapevolezza del pubblico e dei titolari del trattamento in materia di protezione dei dati personali, con particolare attenzione alla tutela dei minori;
- tenere registri interni delle violazioni più rilevanti e imporre sanzioni pecuniarie ove previsto dal Regolamento e dalla normativa nazionale;
- coinvolgere, ove previsto, i cittadini e tutti i soggetti interessati con consultazioni pubbliche dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale.

Il Garante per la protezione dei dati personali è un **organo collegiale**, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile.

L'**Ufficio** del Garante, al quale sovrintende il Segretario generale, coadiuvato da un vice-segretario generale, è attualmente articolato in dipartimenti e servizi, dei quali si indica - in sintesi - l'ambito di attività:

- **Segretario Generale** - coordina l'attività dei dipartimenti e dei servizi e dei dirigenti
- **Dipartimenti**
  - Dipartimento realtà economiche e produttive - *Cura l'esame degli affari riguardanti i trattamenti di dati personali effettuati da soggetti privati con particolare riguardo all'ambito economico e produttivo.*
  - Dipartimento realtà pubbliche - *Cura l'esame degli affari riguardanti i trattamenti di dati personali effettuati da autorità e organismi pubblici, ivi compresi, l'istruzione e la formazione, l'attività degli ordini professionali, a esclusione dei trattamenti che ricadono nell'ambito di applicazione della Direttiva (UE) 2016/680.*
  - Dipartimento sanità e ricerca - *Cura l'esame degli affari riguardanti i trattamenti di dati personali effettuati in ambito sanitario da esercenti le professioni sanitarie e organismi sanitari pubblici e privati, per finalità di cura e amministrative.*
  - Dipartimento reti telematiche e marketing - *Cura l'esame degli affari relativi ai trattamenti di dati nel sistema delle reti telematiche e del commercio elettronico; in tali ambiti provvede agli adempimenti necessari per lo svolgimento dell'attività preliminare ed istruttoria, anche in occasione di attività ispettive, in collaborazione con il dipartimento attività ispettive.*
  - Dipartimento libertà di manifestazione del pensiero e cyberbullismo - *Cura l'esame degli affari relativi ai trattamenti di dati effettuati nel sistema della comunicazione e delle telecomunicazioni, con riferimento agli atti di cyberbullismo o aventi comunque contenuti offensivi o lesivi della dignità di un minore. Cura l'istruttoria degli affari riguardanti l'esercizio del cd. diritto all'oblio, nonché i trattamenti di dati personali effettuati nell'ambito delle manifestazioni del pensiero e dell'esercizio dell'attività giornalistica anche sul web.*
  - Dipartimento risorse umane e attività contrattuali - *Cura la gestione e il trattamento giuridico-economico del personale dipendente e di quello utilizzato ad altro titolo dall'Ufficio; svolge attività di supporto in materia di organizzazione dell'Ufficio e del lavoro; cura le relazioni sindacali e collabora con la competente struttura in materia di contenzioso del personale; elabora il programma annuale di formazione interna d'intesa con le altre unità organizzative e cura la formazione e l'aggiornamento del personale dell'Ufficio, inoltre, cura l'attività negoziale dell'Ufficio e quella in materia di procedure contrattuali.*
  - Dipartimento amministrazione, patrimonio e contabilità - *Cura l'amministrazione e la gestione contabile dell'Ufficio; svolge le altre funzioni previste dal regolamento concernente la gestione amministrativa e la contabilità del Garante; provvede alla conservazione dei beni patrimoniali dell'Ufficio ed al servizio interno di cassa.*
  - Dipartimento attività ispettive - *Nell'ambito dei poteri di indagine disciplinati dall'art. 58 del RGPD, cura lo svolgimento delle attività ispettive e di accertamenti in loco di competenza; svolge altresì, nell'ambito dell'assistenza reciproca con le altre autorità di controllo, o su richiesta, le ispezioni e le indagini previste dall'art. 61 del RGPD; presta la collaborazione richiesta dall'autorità giudiziaria, cura i rapporti con le forze di polizia che cooperano con l'Autorità, ed esegue le indagini per le violazioni costituenti reato che si riferiscono alle materie di competenza del Garante; cura l'attuazione dei protocolli per le relazioni istituzionali connessi all'attività di accertamento e controllo, e i contatti con le competenti amministrazioni e le relative articolazioni sul territorio; Svolge indagini previste dall'art. 57, par. 1, lett. f) del RGPD anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica; cura l'istruttoria per l'applicazione delle sanzioni amministrative pecuniarie in relazione ai casi di negato accesso in violazione dell'articolo 58, par. 1, lett. f)*

del RGPD.

- Dipartimento tecnologie digitali e sicurezza informatica - *Cura il funzionamento e lo sviluppo dei sistemi informativi dell'Ufficio, promuove l'acquisizione e cura l'ordinata gestione dei beni e servizi a contenuto tecnologico.*
- Dipartimento affari legali e di giustizia - *Cura la trattazione degli affari legali dell'Autorità, con specifico riguardo al contenzioso derivante dall'impugnazione di atti e provvedimenti dell'Autorità, di gestione o relativi alle materie di competenza istituzionale; cura la difesa della medesima in caso di impugnazione dell'ordinanza ingiunzione in sede giudiziaria; si occupa dei trattamenti di dati personali connessi all'attività forense, nonché dei trattamenti effettuati presso forze di polizia, uffici giudiziari, organi di autogoverno di magistrature e il Ministero della giustizia.*
- Dipartimento intelligenza artificiale - *Per i profili di carattere giuridico, monitora i fondamenti e la metodologia di progettazione, sviluppo e impiego di sistemi informatici basati su tecnologie di intelligenza artificiale e di apprendimento automatico - c.d. machine learning; segue le iniziative, anche da parte di enti di ricerca, e i tavoli di lavoro nazionali, europei e internazionali con riguardo alle aree di interazioni tra intelligenza artificiale e diritto alla protezione dei dati personali.*

- **Servizi**
  - Servizio affari legislativi e istituzionali - *Monitora l'attività legislativa e regolamentare del Parlamento e del Governo; cura l'istruttoria, anche interna, per la predisposizione degli schemi dei pareri richiesti dal Parlamento, dal Presidente del Consiglio dei ministri e da ciascun Ministro sulle proposte di legge e sugli atti normativi di natura regolamentare basati su atti legislativi; cura i rapporti istituzionali con soggetti pubblici o di interesse collettivo, con riferimento all'attività normativa, anche partecipando a riunioni esterne.*
  - Servizio relazioni internazionali e con l'Unione europea - *Cura le relazioni con gli organismi dell'Unione europea, il Consiglio d'Europa, l'O.C.S.E. ed altre organizzazioni internazionali su questioni d'interesse del Garante ed assicura la partecipazione dell'Ufficio nei comitati e gruppi di lavoro che trattano questioni di competenza dell'Autorità.*
  - Servizio relazioni esterne e media - *Cura le relazioni dell'Autorità con i mezzi di comunicazione e provvede alla diffusione delle informazioni relative all'attività istituzionale del Garante, promuove iniziative editoriali o di informazione di carattere generale o specializzata, mediante campagne informative e la predisposizione di documentazione divulgativa per settori; coordina l'attività informativa sui social media; cura la Newsletter dell'Autorità, la rassegna stampa nazionale ed estera - cartacea, radio-tv e web.*
  - Servizio studi e documentazione - *Effettua studi e ricerche su materie di interesse dell'Autorità anche in riferimento al contesto internazionale, alle nuove tecnologie e ai diritti della personalità, e pone a disposizione, anche di propria iniziativa, pareri e materiale utile specie in relazione a determinate iniziative in corso o a specifiche problematiche da affrontare o a schemi di provvedimento.*
  - Servizio controllo di gestione - *Organizza la raccolta delle informazioni rilevanti relative alle attività del Garante ed ai procedimenti interni; cura la relativa raccolta al fine di assicurare una completa informazione, anche di carattere statistico, sulle medesime attività al fine di garantire un adeguato controllo sulla gestione complessiva dell'Ufficio.*
  - Servizio relazioni con il pubblico - *Cura, anche mediante un servizio di ascolto telefonico o attraverso la posta elettronica, l'informazione al pubblico sulle disposizioni in materia di diritto alla protezione dei dati personali e sulle relative modalità di tutela (segnalazioni e reclami); risponde a quesiti, richieste di informazioni e pareri da parte di cittadini, amministrazioni pubbliche, associazioni o imprese.*

Fanno parte dell'Ufficio anche un:

- Responsabile della segreteria del Collegio;
- Responsabile della protezione dei dati (RPD);
- Responsabile della prevenzione della corruzione e della trasparenza;
- Responsabile per la transizione digitale.

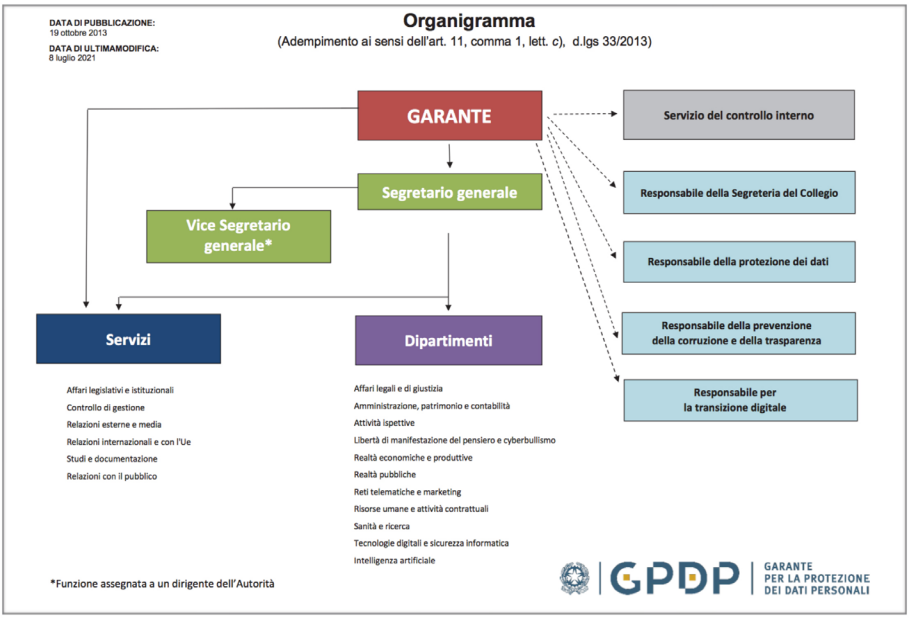


Figura 1 - Organigramma Garante

Capitolo 2

Gli “attori” principali del trattamento

2.1 TITOLARE, CONTITOLARI E RESPONSABILE - ALCUNE CONSIDERAZIONI

I concetti di titolare del trattamento, contitolare e responsabile del trattamento svolgono un ruolo cruciale nell'applicazione del RGPD, in quanto stabiliscono chi è responsabile del rispetto delle diverse norme in materia di protezione dei dati e in che modo gli interessati possono esercitare i propri diritti in concreto.

Svolgiamo ora un approfondimento su questi concetti fondamentali.

Titolare del trattamento (definito dall'art.4 punto 7 del RGPD)

In linea di principio non vi sono limitazioni per quanto concerne la **natura dei soggetti** che possono assumere il ruolo di titolare del trattamento, tuttavia in pratica è solitamente l'organizzazione in quanto tale e non una persona fisica all'interno dell'organizzazione (come l'amministratore delegato, un dipendente o un membro del consiglio di amministrazione) ad agire in qualità di titolare del trattamento.

In rari casi, potrebbe trattarsi di un'organizzazione, ma anche di un singolo o di un gruppo di persone (es. una comunità religiosa può agire come titolare del trattamento, insieme ai singoli membri). Per quanto riguarda il trattamento all'interno di un gruppo di società, occorre prestare particolare attenzione alla questione se uno stabilimento (art.4 punto 16 RGPD) possa agire in qualità di titolare o di responsabile del trattamento, ad esempio quando tratta dati per conto della società controllante.

Talvolta le società e gli organismi pubblici designano una persona specifica quale responsabile dell'esecuzione dell'attività di trattamento. Anche se viene designata una persona fisica specifica per garantire il rispetto delle norme in materia di protezione dei dati, tale persona non sarà il titolare del trattamento, ma agirà per conto del soggetto giuridico (società o organismo pubblico) che risponderà in ultima istanza, in caso di violazione delle norme, in qualità di titolare del trattamento. Nella stessa ottica, anche se un determinato dipartimento o unità all'interno di un'organizzazione ha la responsabilità operativa di garantire la conformità di determinate attività di trattamento, ciò non significa che tale dipartimento o unità (anziché l'organizzazione nel suo insieme) assuma il ruolo di titolare del trattamento.

Esempio

Il dipartimento marketing della società ABC lancia una campagna pubblicitaria per promuovere i suoi prodotti. Il dipartimento decide in merito alla natura della campagna, ai mezzi da utilizzare (e-mail, social media...), ai clienti ai quali rivolgersi e ai dati da utilizzare per ottenere il miglior risultato possibile. Anche se il dipartimento marketing ha agito con notevole indipendenza, in linea di principio la società ABC sarà considerata titolare del trattamento, visto che la campagna pubblicitaria è avviata da tale società e si svolge nell'ambito delle sue attività commerciali e per le sue finalità.

In linea di principio, si può presumere che qualsivoglia trattamento di dati personali da parte dei dipendenti nell'ambito delle attività di un'organizzazione abbia luogo sotto il controllo di quest'ultima; quindi, ai sensi dell'articolo 29 del RGPD, i dipendenti aventi accesso ai dati personali all'interno di un'organizzazione non sono considerati "titolari" o "responsabili" del

trattamento, bensì persone che "agiscono sotto l'autorità del titolare del trattamento o del responsabile del trattamento". In circostanze eccezionali, tuttavia, può avvenire che un dipendente decida di utilizzare i dati personali per finalità proprie, andando così illegittimamente oltre l'autorità conferitagli.

Il titolare del trattamento è il soggetto che **decide** in merito a determinati elementi chiave del trattamento stesso. La titolarità può essere definita a norma di legge o può derivare da un'analisi degli elementi di fatto o delle circostanze del caso.

Occorre studiare le specifiche operazioni di trattamento in questione e capire chi le determina, ponendosi per es. le seguenti domande: *Perché il trattamento ha luogo? e Chi ha deciso che il trattamento debba avvenire per una determinata finalità?* Si possono, pertanto, distinguere due categorie di situazioni:

1. titolarità derivante da **disposizioni giuridiche**;
2. titolarità derivante da un'**influenza concreta**.

Nel primo caso, il fatto che la titolarità del trattamento sia stata definita specificamente per legge sarà determinante per stabilire chi agisce in quanto titolare. La legislazione nazionale prevede che le autorità pubbliche siano responsabili del trattamento dei dati personali nell'ambito delle rispettive competenze. Tuttavia, più comunemente, anziché designare direttamente il titolare del trattamento o stabilire i criteri per la sua designazione, la legge definisce un compito o impone l'obbligo di raccogliere e trattare determinati dati. In tali casi, la finalità del trattamento è spesso determinata per legge. Il titolare del trattamento è di norma il soggetto cui la legge demanda la realizzazione di tale finalità, di tale funzione pubblica.

Esempio - situazione 1

La legislazione nazionale del paese A prevede l'obbligo per le autorità comunali di erogare prestazioni sociali quali versamenti mensili ai cittadini in base alla loro situazione finanziaria. Per effettuare tali pagamenti, l'amministrazione comunale deve acquisire ed elaborare dati sulla situazione finanziaria dei richiedenti. Anche se non è previsto esplicitamente dalla legge, le autorità comunali sono i titolari di tale trattamento in virtù, implicitamente, delle disposizioni giuridiche.

Nel secondo caso, in assenza di titolarità derivante da disposizioni giuridiche, la qualifica di titolare del trattamento deve essere stabilita sulla base di una valutazione delle circostanze concrete del trattamento; ossia di una valutazione "fattuale". La necessità di una valutazione fattuale significa che la titolarità di un trattamento non deriva dalle caratteristiche soggettive di chi tratta i dati, ma dalle attività concretamente svolte da tale soggetto in un contesto specifico. In altre parole, uno stesso soggetto può agire contemporaneamente in qualità di titolare del trattamento per determinate operazioni di trattamento, e in qualità di responsabile del trattamento per altre operazioni. Quindi, la qualifica di titolare o di responsabile del trattamento va valutata in relazione a ciascuna specifica attività di trattamento dei dati.

Esempio - situazione 2

- **Studi Legali:** la società ABC si rivolge a uno studio legale per rappresentarla in una controversia. Per svolgere tale compito, lo studio legale è tenuto a trattare i dati personali relativi alla causa. Il trattamento dei dati personali è motivato dal mandato dello studio legale di rappresentare il cliente in tribunale. Detto mandato, tuttavia, non riguarda specificamente il trattamento dei dati personali. Lo studio legale agisce con un grado significativo di indipendenza, ad esempio nel decidere quali informazioni utilizzare e come utilizzarle e non vi sono istruzioni della società cliente in merito al trattamento dei dati personali. Il trattamento effettuato dallo studio per svolgere il compito di rappresentante legale della società è pertanto legato al ruolo funzionale dello studio stesso, che deve essere considerato titolare del trattamento.
- **Operatori di telecomunicazioni:** la fornitura di un servizio di comunicazione elettronica, come la posta elettronica, comporta il trattamento di dati personali. Il fornitore di tali servizi sarà di norma considerato titolare del trattamento dei dati personali necessari per il funzionamento del servizio in quanto tale (ad esempio, dati relativi al traffico e alla fatturazione). Se l'unica finalità e ruolo del fornitore è quello di consentire la trasmissione di messaggi di posta elettronica, il fornitore non sarà considerato titolare del trattamento per quanto riguarda i dati personali contenuti nel messaggio stesso. Il titolare del trattamento dei dati personali contenuti nel messaggio è di norma la persona da cui proviene il messaggio, piuttosto che il prestatore di servizi che offre il servizio di trasmissione. *[L'EDPB ritiene che questo esempio, precedentemente contemplato al considerando 47 della direttiva 95/46/CE, continui a essere pertinente anche ai sensi del RGPD].*
- **Servizio standardizzato di archiviazione su cloud:** un grande fornitore di servizi di archiviazione su cloud offre ai propri clienti la possibilità di archiviare volumi ingenti di dati personali. Il servizio è completamente standardizzato e i clienti hanno scarsa o nessuna capacità di personalizzarlo. I termini contrattuali sono stabiliti e redatti unilateralmente dal fornitore di servizi cloud e forniti al cliente in un'ottica di «prendere o lasciare». La società X decide di avvalersi del fornitore di servizi cloud per archiviare dati personali relativi ai propri clienti. La società X continuerà a essere considerata titolare del trattamento, alla luce della sua decisione di avvalersi di questo fornitore specifico di servizi cloud per trattare dati personali per le proprie finalità. Nella misura in cui il fornitore di servizi cloud non tratti i dati personali per le proprie finalità e li archivi esclusivamente per conto dei propri clienti e conformemente alle istruzioni, il fornitore di servizi sarà considerato responsabile del trattamento.

Talune attività di trattamento possono essere considerate come naturalmente connesse al ruolo ricoperto da un determinato soggetto (il datore di lavoro rispetto ai dipendenti, l'editore rispetto agli abbonati o un'associazione rispetto ai membri). In molti casi, le condizioni previste da un contratto possono agevolare l'individuazione del titolare del trattamento, sebbene non siano sempre determinanti.

Se una parte decide di fatto le finalità e le modalità del trattamento di dati personali, essa sarà il titolare del trattamento anche laddove un contratto la indichi come responsabile di tale trattamento. Analogamente, non è sufficiente che un contratto designi una parte come "subappaltatore" affinché tale parte contrattuale sia considerata responsabile del trattamento ai sensi della normativa in materia di protezione dei dati. Anche se il responsabile del trattamento offre un servizio definito in via preliminare in modo specifico, al titolare del trattamento deve essere messa a disposizione una descrizione dettagliata di tale servizio e spetta al titolare