3 Atti Convegni

Nicola Galotta

Individuare i dati trattati ed i principali soggetti coinvolti nei trattamenti

D*urante il Convegno nazionale di studio AGIDAE, svoltosi a Roma il 20 ottobre 2018, si è svolto l'intervento dell'Ing. Nicola Galotta dal titolo* ***"L'applicazione della normativa Privacy nelle diverse attività degli Enti: scuola, attività socio-sanitaria- assistenziale, ricettività, uffici****".*
Di seguito si riporta la relazione sull'argomento trattato.

****

Prima di addentrarsi nell'organizzazione del sistema Privacy e nei relativi adempimenti è opportuno chiedersi cosa s'intende per dati personali e per trattamento e quali sono le figure principali coinvolte nel trattamento.

Dati personali e loro trattamento

Secondo l'art. 4 del GDPR, un **dato personale** è "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".
È da precisare che, i principi di protezione dei dati non si applicano ad informazioni

anonime; vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Inoltre non si applicano ai dati personali delle persone decedute.

All'interno dei dati personali ci sono alcune *categorie particolari di dati,* quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni relative al suo stato di salute, o alla vita sessuale o all'orientamento sessuale della persona.
Per queste categorie particolari di dati i principi e le misure di protezione dei dati richiesti dal GDPR sono più stringenti.

Un esempio, non esaustivo, di dati personali, generalmente raccolti in:

- contratti di lavoro, schede per l'iscrizione/accoglienza/accettazione relative ad alunni, genitori, ospiti di attività ricettive, pazienti;
- registro personale del docente, registro di classe, documentazione relativa alla programmazione didattica, documenti di valutazione alunni, elaborati, piani didattici personalizzati;
- certificati medici riportanti prescrizioni, diagnosi ed altri elementi atti a stabilire lo stato di salute;
- corrispondenza con famiglie e pazienti (elettronica e cartacea);
- atti o documenti giudiziari relativi a condanne penali e reati (es. riferite ad alunni, a genitori di alunni, a pazienti).

Identificativi	Particolari	Giudiziari
- nome e cognome; - data di nascita e luogo di nascita; - indirizzo di casa; - recapiti telefonici e di posta elettronica; - codice fiscale; - numero di tessera sanitaria, carta d'identità, passaporto, patente; - numero di targa del veicolo; - numeri di carta di credito; - professione, titolo di studio; - identità digitale; - account name o nickname; - indirizzo IP di dispositivi fissi e mobile (quando collegato ad altri dati identificativi); - filmati e foto di video	- origine razziale o etnica (info non rilevabile dal solo luogo di nascita o dal nome); - opinioni politiche; - le convinzioni religiose o filosofiche (info rilevabile ad esempio dalla scelta scolastica per le ore di religione); - relativi alla vita sessuale o all'orientamento sessuale della persona; - appartenenza sindacale (info rilevabile ad esempio dal cedolino paga); - dati relativi allo stato di salute; - informazioni genetiche (info ad esempio derivabile da	- documenti e informazioni che rivelano l'esistenza di provvedimenti penali suscettibili di iscrizione nel casellario giudiziale, o la qualità di indagato o imputato.

Identificativi	Particolari	Giudiziari
sorveglianza e/o attività didattiche/ludico-ricreative.	documentazione sanitaria); - documentazione relativa ad alunni con DSA (può rivelare lo stato di salute/la diagnosi specifica di un individuo identificabile); - biometrici intesi a identificare in modo univoco una persona fisica ad esempio: impronte digitali o calligrafia (info rilevabile ad es. dai sistemi di controllo accessi o marcatori orario o per sbloccare l'accesso a smartphone di ultima generazione ed a computer); - qualunque tipo di indicazione relativa, per esempio, all'eventuale rischio di malattia, o a qualunque tipologia di disabilità e malattia, ad anamnesi mediche, stati fisiologici e trattamenti clinici, a prescindere dalla fonte (sia essa un ospedale, un medico, un operatore sanitario, un test diagnostico oppure un dispositivo medico); - qualunque tipo di informazione, fornita dallo stesso soggetto, durante una registrazione volta a ricevere qualunque tipo di assistenza sanitaria o prestazione medica; - qualunque dato riguardante una persona fisica e che è utilizzato per l'identificazione di quest'ultima in modo assolutamente univoco per il sistema sanitario; - qualunque informazione determinata da controlli oppure esami clinici effettuati o su una sostanza organica o direttamente su una parte del corpo, inclusi campioni biologici e dati genetici.	

Secondo l'art. 4 del GDPR, il «**trattamento**» di dati personali è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. In altre parole il trattamento è una qualsiasi operazione che si fa con i dati personali. La semplice

raccolta/richiesta all'interessato dei suoi dati è da considerarsi un trattamento, così come la conservazione, l'uso e la comunicazione dei dati sono un trattamento.

Inoltre intendiamo per «**finalità del trattamento**» lo scopo per il quale effettuiamo il trattamento dei dati personali (motivo di raccolta ed uso). Alcuni esempi (non esaustivi) di finalità del trattamento di dati personali raccolti da Clienti, suddivisi per tipologie di attività:

Accoglienza	Scuola	Socio Assistenziale
Comunicare alla Questura le generalità dei clienti alloggiati.	Istruzione e formazione degli alunni ed attività amministrative ad esse strumentali, così come definite dalla normativa vigente.	Gestione del rapporto con gli utenti e i loro familiari o rappresentanti per l'erogazione di prestazioni di prevenzione, diagnosi, cura e riabilitazione e di prestazioni socio sanitarie.
Attività ed obblighi amministrativi, contabili e fiscali inerenti ai servizi offerti agli ospiti.	Comunicazione a soggetti pubblici (quali, ad esempio, ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) nei limiti di quanto previsto dalle vigenti disposizioni di legge.	Gestione amministrativa connessa all'erogazione di prestazioni socio sanitarie.
Funzione di ricevimento di comunicazioni, messaggi e telefonate indirizzate agli ospiti.	Comunicazione a terzi per l'organizzazione e gestione di gite scolastiche, viaggi d'istruzione e campi scuola.	Erogazione di servizi assistenziali, infermieristici, fisioterapici, medici e sanitari.
Accelerare le procedure di registrazione in caso di successivi soggiorni presso la struttura.	Comunicazione a terzi in relazione a polizze in materia infortunistica.	Erogazione dei servizi a favore degli interessati in condivisione o in contitolarità con altri soggetti (medici, farmacisti, liberi professionisti, operatori servizi sociali, enti territoriali, ecc.).
Invio di messaggi promozionali su tariffe e offerte.	Erogazione servizio mensa.	Analisi statistiche o attività di ricerca (mediante dati anonimi).
Tenuta del fascicolo personale per la raccolta di documenti e registri relativi alla vita lavorativa dei dipendenti.	Pubblicazione sul sito istituzionale e/o sul giornalino e/o sull'annuario della scuola di foto di classe, di lavori e di attività didattiche afferenti ad attività istituzionali della scuola inserite nel Piano dell'Offerta Formativa (quali ad esempio foto relative ad attività di laboratorio, visite guidate, premiazioni, partecipazioni a gare sportive, ecc.).	Tenuta del fascicolo personale per la raccolta di documenti e registri relativi alla vita lavorativa dei dipendenti.

Accoglienza	Scuola	Socio Assistenziale
Amministrazione del rapporto di lavoro (stipendi, pagamenti, comunicazioni ad Enti preposti).	Compilazione e gestione di documenti di valutazione e orientamento degli alunni raccolti nel "Portfolio delle competenze individuali".	Amministrazione del rapporto di lavoro (stipendi, pagamenti, comunicazioni ad Enti preposti).
Gestione dei contratti di fornitura/appalti.	Tenuta del fascicolo personale per la raccolta di documenti e registri relativi alla vita lavorativa dei lavoratori.	Gestione dei contratti di fornitura/appalti.
Obblighi amministrativi, contabili e fiscali derivanti da contratti di fornitura/appalti. Etc.	Amministrazione del rapporto di lavoro (stipendi, pagamenti, comunicazioni ad Enti preposti).	Obblighi amministrativi, contabile e fiscali derivanti da contratti di fornitura/appalti. Etc.

Principali soggetti coinvolti nel trattamento

In base alle definizioni dell'art. 4 del GDPR, analizziamo le principali figure coinvolte nel trattamento dei dati.

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**". Le responsabilità ed il ruolo del titolare del trattamento vengono disciplinate nell'art. 24 del GDPR.

In sostanza il "titolare del trattamento" è colui che decide sia le ragioni che le modalità del trattamento dei dati senza ricevere istruzioni da altri e senza dover rendere conto a terzi che non siano gli interessati.

In linea generale il **titolare è individuato nel vertice dell'azienda, ovvero la società, l'ente o l'associazione nel suo complesso**.

Nell'ambito di una persona giuridica il **titolare del trattamento si identifica nell'ente/soggetto nel suo complesso** anziché in taluna delle persone fisiche che operano nella relativa struttura (superiori, direttori, amministratori, ecc.) e che concorrono in concreto ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, il legale rappresentante, ecc.), secondo gli statuti e il diritto proprio.

Nel mondo degli Enti Religiosi il titolare del trattamento è tipicamente l'Ente Ecclesiastico. La persona fisica con cui interloquire, che fa da tramite con il soggetto giuridico, potrebbe essere il legale rappresentante o persona da questi delegata.

All'interno dell'organizzazione sia del titolare che del responsabile si trovano le **persone autorizzate al trattamento** (ex *incaricati*). Esse sono le persone fisiche

che elaborano o utilizzano materialmente i dati personali sulla base delle istruzioni ricevute dal titolare e/o dal responsabile.

Alcuni esempi (non esaustivi) di persone autorizzate al trattamento di dati personali raccolti da interessati, suddivisi per tipologie di attività, sono:

Accoglienza	Scuola	Socio Assistenziale
Addetto all'accoglienza / Receptionist. Addetto amministrativo.	Coordinatori Didattici. Docenti. Addetti alla segreteria didattica. Addetti amministrativi. Cuoca (limitatamente all'eventuale trattamento di diete/certificazioni che possano rappresentare lo stato di salute di una persona identificabile).	Direttore Sanitario. Medico. Addetto all'accettazione. Addetto amministrativo.

L'autorizzazione al trattamento per questi soggetti e quindi la loro responsabilizzazione deve avvenire attraverso una specifica lettera di incarico. La lettera dovrà contenere:

- Le finalità ed i trattamenti autorizzati.
- Categorie di dati.
- Categorie di interessati.
- Le istruzioni operative da utilizzare.
- Le misure di sicurezza da utilizzare.
- Il richiamo all'obbligo di riservatezza.

Il «**responsabile del trattamento**» è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento**".

Per poter delineare meglio la figura del responsabile del trattamento e quindi individuare il soggetto a cui è attribuibile questo ruolo, vanno analizzati alcuni degli aspetti significativi previsti dall'art. 28 del GDPR (responsabile del trattamento).

Il titolare del trattamento, prima di designare un responsabile e di affidargli l'incarico, deve verificarne le caratteristiche, le competenze e assicurarsi che offra garanzie sufficienti per ricoprire il ruolo e sia in grado di adottare misure tecniche e organizzative adeguate a tutelare i diritti degli interessati.

I trattamenti effettuati dal responsabile devono essere disciplinati da un contratto o da un atto giuridico che vincoli il responsabile al titolare e che delinei gli accordi

stabiliti tra i due attori. L'accordo dovrà contenere una descrizione dettagliata delle attività da svolgere (tipologia dei dati personali trattati, finalità e durata del trattamento, obblighi e diritti del titolare) e dovrà prevedere che il responsabile possa effettuare le attività di trattamento esclusivamente dietro istruzione documentata del titolare, soprattutto in caso di trasferimento dei dati personali verso un'organizzazione internazionale o un paese terzo.
Il responsabile dovrà garantire che le persone autorizzate a trattare i dati personali abbiano un impegno alla riservatezza e dovrà impegnarsi a non affidare ad altri responsabili specifiche attività di trattamento senza la preventiva autorizzazione del titolare. Il responsabile designato dal titolare conserva nei confronti di quest'ultimo l'intera responsabilità dell'adempimento degli obblighi degli altri responsabili nel caso di loro inadempienza. Titolare e responsabile hanno diverse attribuzioni ma obblighi condivisi.
La figura del responsabile del trattamento prevista dal GDPR è profondamente diversa da quella delineata dall'art. 29 del Codice della Privacy Italiano. L'art. 29 era chiaramente rivolto a figure interne all'organizzazione, viste come sub-responsabili o soggetti intermedi tra il titolare e gli incaricati al trattamento. L'art. 29 del Codice della Privacy Italiano oggi è abrogato.
L'ambito applicativo dell'art. 28 del GDPR delinea come destinatario il soggetto al quale vengono delegati uno o più trattamenti di dati. Le garanzie e le autonomie richieste al responsabile del trattamento previste dal comma 1 dell'art. 28, l'autorizzazione per il trattamento prevista dal comma 2 dell'art. 28, il fatto che i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico (comma 3 dell'art. 28), il concetto di codice di condotta e di meccanismo di certificazione previsto invece dal comma 5 dell'art. 28, l'obbligo della tenuta del registro dei trattamenti previsto dall'art 30 del GDPR, l'impianto sanzionatorio posto anche a carico del responsabile del trattamento, delineano una delega di funzioni da parte del titolare al responsabile del trattamento difficilmente compatibile e/o applicabile con l'autonomia e la discrezionalità propria di una figura interna all'organizzazione, specialmente se dipendente.

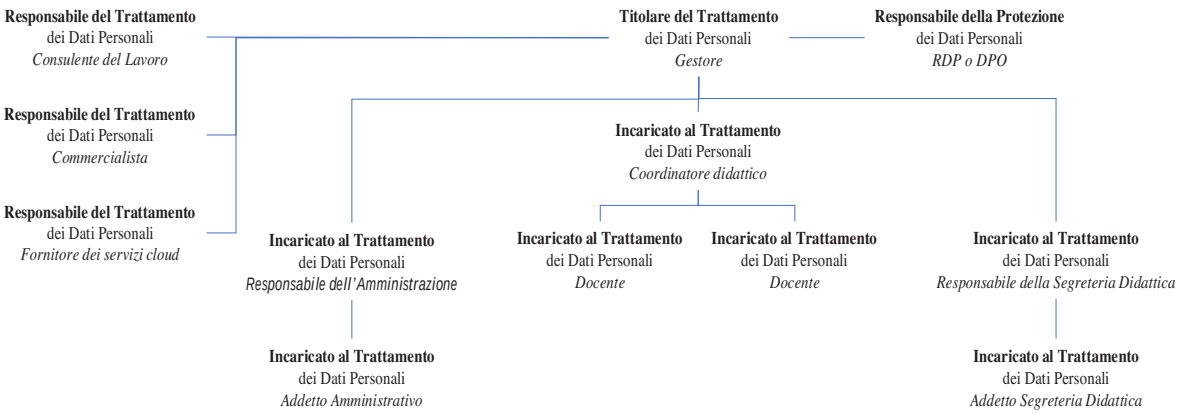
Quindi, **il ruolo del responsabile del trattamento di cui al regolamento europeo è essenzialmente riservato ad un soggetto esterno all'azienda, con riferimento ai fornitori di servizi**, che attenendosi alle istruzioni del titolare, assume responsabilità proprie e ne risponde alle autorità di controllo e alla magistratura. Il titolare del trattamento può distribuire incarichi interni (es. responsabile dell'area legale, dell'area marketing, ecc.), ma la responsabilità rimane del titolare.
Per l'identificazione del soggetto Responsabile del Trattamento, in via del tutto esemplificativa, si potrebbe seguire la regola di individuare il responsabile

nell'ambito del subappalto a terzi di porzioni di attività che concorrono ad erogare il servizio in via diretta e/o indiretta e che in assenza di subappalto il titolare dovrebbe svolgere in proprio. Essendo il subappalto regolato da un contratto di servizio, lo stesso contratto dovrà contenere le specifiche relative al trattamento congiuntamente stabilite, per cui in questo caso non sono previste ulteriori lettere specifiche per l'incarico di Responsabile al Trattamento dei Dati.

Nel settore degli Enti Religiosi i ***Responsabili del trattamento dei dati*** *sono tipicamente: lo studio di consulenza del lavoro, la società esterna che si occupa dei servizi di mensa (qualora riceva dati personali), la società di manutenzione dei software gestionali in cloud, registro elettronico in cloud, servizi digitali remoti, ecc.*

Il GDPR prevede ulteriori figure per la protezione dei dati, tuttavia non tutte sono generalmente applicabili al settore degli Enti Religiosi (come ad es. il ***Responsabile della Protezione dei Dati***, altresì detto RPD oppure usando l'acronimo inglese DPO o erroneamente detto Responsabile della Privacy) e per le quali si rimanda a più specifiche trattazioni.

La figura successiva mostra un'ipotesi di distribuzione delle figure della privacy, precedentemente illustrate, nel caso della Scuola:



Per agevolare gli Enti nell'applicazione del GDPR, **Agidae Opera** mette a disposizione un servizio di consulenza che ha l'obiettivo di formare e accompagnare gli Istituti nella revisione e nella predisposizione di quanto previsto dal GDPR e dal Codice della Privacy.