TRATTAMENTO DEI DATI PERSONALI

Guida alla lettura delle disposizioni in materia di trattamento di dati personali (rev. 2023)

Regolamento (UE) 679/2016

D.Lgs. 196/2003 Codice in materia di trattamento dei dati personali

Università degli studi di Catania
Responsabile protezione dei dati

Sommario

Il REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI 679/2016

Premessa

Il Regolamento (UE) 2016/679 (*General Data Protection Regulation* – GDPR), "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", pienamente efficace dal 25 maggio 2018, armonizza la normativa in materia di protezione dei dati personali all'interno dell'Unione Europea; rappresenta l'impegno da parte dei governi europei a garantire che i dati personali dei loro cittadini siano adeguatamente protetti in tutto il mondo.

Il Regolamento pone al centro dell'attenzione la tutela della persona umana, delle sue libertà e della sua dignità e il rafforzamento dei diritti fondamentali dei cittadini europei nell'era digitale.

Vista la natura regolamentare della norma, non necessita di recepimento da parte dei Paesi UE ed è attuata allo stesso modo in tutti gli Stati dell'Unione.

Il GDPR, introducendo una serie di novità in ambito di trattamento di dati personali e di sicurezza del trattamento, modifica il concetto di adempimento *privacy* a cui si era abituati. Il trattamento non è più soggetto a regole dettagliate e circostanziate e ad adempimenti formali; il Regolamento europeo lascia al Titolare ampio potere decisionale, imponendogli, però, un percorso di adeguamento (*compliance*) efficace, basato sulla minimizzazione del rischio e sul controllo del dato da parte dell'interessato.

Il D.Lgs. 196/2003 - Codice in materia di trattamento dei dati personali, non è stato abrogato, ma adeguato e integrato dal D.Lgs. 101/2018, entrato in vigore il 19 settembre 2018, con la funzione di armonizzare le disposizioni del Codice con quelle introdotte dal Regolamento.

Il D. L. 2021/139 ha portato ulteriori modifiche al "Codice privacy".

Il nuovo *Codice Privacy* italiano introduce rilevanti novità riguardo i codici deontologici, le regole di condotta, il trattamento di "categorie particolari di dati" per finalità di ricerca scientifica, fini statistici, ricerca storica e di rilevante interesse pubblico, l'accesso ai documenti amministrativi e la fatturazione elettronica; prevede importanti modifiche riguardo le sanzioni, i diritti dell'interessato, l'utilizzabilità dei dati acquisiti in violazione delle disposizioni e attribuisce al Garante poteri più forti e ulteriori compiti.

Quindi, a partire da settembre 2018, ogni pubblica amministrazione, ente o società di servizi, impresa o struttura di ricerca e di studio, è tenuta a dare piena e integrale applicazione a tutta la normativa effettuando un percorso di conformità alle norme, alle regole, agli standard della normativa europea.

Il Regolamento chiama tutti ad un approccio concettuale innovativo che prevede, già dalla programmazione di una procedura (didattica, amministrativa o scientifica), il rispetto dei principi fondamentali e l'utilizzo di strumenti e mezzi idonei ed atti a garantire che il rischio di impatti negativi sulle libertà e sui diritti degli interessati sia minimizzato.

La non conformità e la violazione delle norme in materia di protezione dei dati espongono l'Ateneo al rischio di sanzioni giudiziarie o amministrative e danni alla reputazione.

Questa Guida, senza alcuna pretesa di esaustività, nasce allo scopo di offrire una prima lettura semplificata delle principali disposizioni dettate dal GDPR, anche alla luce della nuova declinazione del Codice di protezione dei dati (D.Lgs. 2003/196).

L'Ufficio per la protezione dei dati è a disposizione delle strutture dell'Ateneo per fornire informazioni o assistenza per un corretto trattamento dei dati personali.

I contatti dell'Ufficio sono pubblicati all'indirizzo: https://www.unict.it/content/privacy

AMBITO DI APPLICAZIONE

Tutela dei dati personali

Il regolamento europeo disciplina il trattamento di dati personali relativi alle persone fisiche, nei paesi UE, da parte di persone, società ed organizzazioni e mira a tutelarli dai rischi di violazione dei diritti e delle libertà fondamentali a cui potrebbero andare incontro.

La norma europea si applica solo ai dati personali delle persone fisiche e non ai dati delle società o di altre persone giuridiche. A tal proposito, bisogna però tenere presente che le informazioni relative alle imprese individuali possono costituire dati personali se consentono l'identificazione di una persona fisica.

Applicazione del Regolamento

Le disposizioni del Regolamento trovano applicazione sia per trattamenti automatizzati che per trattamenti manuali di dati personali. Fra i trattamenti esclusi dal campo di applicazione del Regolamento, si evidenziano quelli effettuati per scopi personali o sulla base di normative extra-UE (i quali saranno disciplinati dalla normativa nazionale), nonché i trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse (disciplinati dal d.lgs. 51/2018).

L'art. 3 del GDPR prescrive, inoltre, l'applicazione del Regolamento anche ai Titolari non stabiliti nell'Unione che offrono servizi e prodotti all'interno del mercato europeo (ad esempio: Google Inc., Facebook Inc., Dropbox Inc.; Twitter Inc.).

DATI PERSONALI

Dati personali e identificativi

I dati personali sono quelli che, da soli o insieme ad altri, consentono l'identificazione di una persona fisica (interessato) o la rendono identificabile, direttamente o indirettamente, nonché quelli che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

I dati personali che permettono l'identificazione diretta sono, ad esempio: dati anagrafici, immagini, voce, ecc.; quelli che consentono l'identificazione indiretta (cioè riguardanti una persona la cui identità può essere comunque accertata mediante informazioni supplementari) sono, ad esempio: codice fiscale, indirizzo IP, numero di targa, cookie, ecc.

Categorie particolari di dati personali (c.d. dati sensibili)

Fra tutti i dati personali, il GDPR specifica che alcuni di essi rientrano in "categorie **particolari di dati personali**", i c.d. "dati sensibili" (origine razziale, opinioni politiche, appartenenza sindacale, convinzioni religiose, orientamento sessuale, ecc.), già previsti dal Codice privacy; fra questi rientrano quelli individuati in particolare all'art. 4 par. dal 12 al 15:

- **Dati genetici -** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **Dati biometrici** - i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **Dati relativi alla salute -** i dati personali attinenti 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 (sia fisica che mentale).

TRATTAMENTI

Definizione di trattamento

Il Regolamento, all'art. 4, precisa che si intende per trattamento la molteplicità di operazioni, applicate a dati personali, sia con strumenti parzialmente o interamente automatizzati che manuali, se parte di un sistema di archiviazione strutturato, quali 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.

Il trattamento non dovrà essere solo necessario e con gli scopi accuratamente definiti, ma soprattutto proporzionato alla finalità del trattamento, per consentire di stabilire quali informazioni sono davvero necessarie e quali, invece, superflue e quindi da non trattare.

Liceità del trattamento (base giuridica)

Il trattamento di dati personali è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni, indicate all'art. 6 del GDPR: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Il Titolare del trattamento, prima di iniziare un trattamento, ha l'obbligo di valutare quale sia la base giuridica più idonea al trattamento che intente effettuare, in relazione ai requisiti di ciascuna delle basi previste dall'art.6 del Regolamento europeo in relazione ai requisiti. Ogni base giuridica, infatti, risponde a condizioni specifiche, e ha differenti conseguenze sui diritti delle persone.

La base giuridica per il trattamento dei dati personali da parte dei soggetti pubblici, come ampliata dal D.L. 2021/139 deve essere costituita da una norma di legge o, nei casi previsti dalla legge, di regolamento o di un atto amministrativo generale

Come definito dalla Cass. civ. Sez. Unite, 28 novembre 1994, n. 10124, si intende per Atto amministrativo generale l'atto espressione di "*potestà amministrativa*", rivolto alla "*cura concreta di interessi pubblici, con effetti diretti nei confronti di una pluralità di destinatari non necessariamente determinati nel provvedimento, ma determinabili*" e che "*esprime una scelta di carattere essenzialmente tecnico, con cui l'amministrazione persegue la cura degli interessi pubblici a essa affidati dalla legge*" (Corte cost., 22 luglio 2010, n. 278).

I trattamenti effettuati dalle Pubbliche amministrazioni

Base giuridica per il trattamento

La base giuridica per il trattamento dei dati personali da parte dei soggetti pubblici, come ampliata dal D.L. 2021/139 deve essere costituita da una norma di legge o, nei casi previsti dalla legge, di regolamento o di un atto amministrativo generale

Come definito dalla Cass. civ. Sez. Unite, 28 novembre 1994, n. 10124, si intende per Atto amministrativo generale l'atto espressione di "*potestà amministrativa*", rivolto alla "*cura concreta di interessi pubblici, con effetti diretti nei confronti di una pluralità di destinatari non necessariamente determinati nel provvedimento, ma determinabili*" e che "*esprime una scelta di carattere essenzialmente tecnico, con cui l'amministrazione persegue la cura degli interessi pubblici a essa affidati dalla legge*" (Corte cost., 22 luglio 2010, n. 278).

Comunicazione e diffusione

Il d.lgs. 196/2003, novellato dal d.lgs. 101/2018 (Codice privacy), all'art. 2-ter par. 4 definisce che:

- "Comunicazione" è il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato o dalle persone autorizzate al trattamento o coinvolte nelle attività di trattamento.
- "Diffusione" è il dare conoscenza dei dati personali a soggetti indeterminati in qualunque forma, anche mediante la loro messa in disposizione o consultazione.

L'art. 2-ter comma 2 stabilisce che "la comunicazione fra Titolari che effettuano trattamenti di dati personali soggetti pubblici, per dati diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1 o se necessaria ai sensi del comma 1-bis

La diffusione dei dati personali è consentita solo se disposta da norma di legge o di regolamento, o se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti. In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento; in tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione

Pertanto, prima di procedere alla diffusione di dati personali o alla pubblicazione sui siti universitari di documenti o atti contenenti dati personali, è necessario verificare che esistano i presupposti normativi che legittimano la diffusione.

La diffusione di dati personali che rivelano stati di salute o esistenza di patologie e condizioni di disabilità fisici che mentali, disabilità, origine razziale e/o altre categorie particolari di dati è vietata.

Trattamento di dati particolari

Il trattamento delle "categorie particolari di dati personali" è sempre vietato, ad esclusione di una delle condizioni elencate al par. 2 dell'art. 9 (esempio: consenso esplicito, diritti del Titolare in materia di diritto del lavoro e sicurezza sociale, ecc.); in questi casi è necessaria una tutela rafforzata sui dati, allo scopo di garantire la libertà e la dignità della persona contro possibili ingerenze sulle decisioni e/o discriminazioni.

A tal proposito, il d.lgs. 196/2003 all'art. 2-sexies specifica che è ammesso il trattamento delle *categorie particolari di dati personali* se necessario per motivi di *interesse pubblico rilevante* qualora siano previsti dal diritto dell'Unione Europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento, che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Profilazione e processo decisionale automatizzato

Il GDPR, all'Art. 4, definisce la profilazione come: "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

Il Cons. 24 chiarisce che, "per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali".

Inoltre, all'art 22, il GDPR stabilisce un divieto generale alla profilazione e ai processi decisionali automatizzati, che producano effetti giuridici sull'interessato o che incidano significativamente sulla sua persona.

Un interessato può essere sottoposto ad un processo decisionale automatizzato, compreso la profilazione, esclusivamente nei casi definiti dall'art.22 par.2 lett. a),b),c), seppur con misure appropriate a tutela dei diritti dell'interessato.

SOGGETTI

Interessato *(data subject)*

L'interessato è la persona fisica, identificata o identificabile, alla quale si riferiscono i dati personali. Può essere solo una persona fisica, e non una persona giuridica, un ente o un'associazione. Nel caso di imprese individuali possono costituire dati personali quelli che consentono l'identificazione di una persona fisica.

L'interessato gode di una serie di specifici diritti nei confronti del Titolare.

Titolare (*data controller*)

Il Titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione che determina singolarmente o insieme ad altri la finalità e i mezzi del trattamento dei dati personali.

Il Titolare del trattamento è quindi l'Ente nel suo complesso (ad esempio: l'università, la società, il ministero, l'ente pubblico, l'associazione, ecc.) e non le persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio: il ministro, il rettore, il direttore generale, il presidente, il legale rappresentante, ecc.).

Il GDPR all'art. 26 prevede la contitolarità del trattamento.

Fra i compiti attribuito dal GDPR al Titolare vi sono:

- adozione delle misure tecniche e organizzative atte a garantire, sin dalla fase della progettazione del servizio da erogare e/o dell'attività da svolgere, la tutela dei diritti dell'interessato (*privacy by design*) e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente, riducendo al minimo il trattamento dei dati personali, mediante misure tecniche/organizzative al fine di dimostrare la conformità con il Regolamento;
- vincolo al **dovere di riservatezza** dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
- designazione del Responsabile del trattamento a cui affidare mansioni importanti e di elevata professionalità, in fase di gestione dei dati personali;
- redazione del **registro di trattamenti**;
- formazione del **personale**;

- documentazione delle **violazione dei dati personal**i, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio;
- notifica al Garante nei casi previsti.

Contitolare (joint controller)

Sono Contitolari di un trattamento di dati personali, quando la scelta delle finalità e delle modalità impiegate per svolgere un trattamento sia determinata in maniera congiunta tra due o più Titolari pubblici o privati, tale che ne deriva una responsabilità congiunta fra (Con)Titolari del trattamento.

Responsabile del trattamento (*data processor*)

Il Responsabile del trattamento è la persona fisica o giuridica, **esterna** alla struttura organizzativa, al quale il Titolare affida specifici e definiti compiti, volti ad effettuare, per proprio conto, il trattamento dei dati; il Responsabile deve fornire garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto, o da altro atto giuridico a norma (*data protection agreement*), che vincolano il Responsabile del trattamento al Titolare del trattamento e che prevede le particolari condizioni riportate all'art. 28 del GDPR.

Responsabile della protezione dei dati (RPD o *Data Protection Officer* – DPO).

Quando il trattamento è effettuato da un Ente pubblico, il Titolare deve designare un Responsabile della protezione dati (RPD) per facilitare l'attuazione della normativa (articoli 37, 38 e 39 GDPR). Il RPD svolge vari compiti, tra i quali: il supporto informativo, la consulenza al Titolare e ai soggetti designati che eseguono il trattamento; la sorveglianza sull'osservanza del trattamento e delle politiche definite dal Titolare sulla protezione dei dati personali; la sensibilizzazione e la formazione del personale; fornire, se richiesto, la formulazione di pareri sulla valutazione di impatto. Inoltre ha la funzione di punto di contatto per gli interessati e per il Garante rispetto a ogni questione attinente l'applicazione del Regolamento.

Soggetti designati (Responsabile interno del trattamento)

Il decreto 196/2003 all'art. 2 - *quaterdecies* precisa che, nell'ambito del proprio assetto organizzativo e sotto la propria responsabilità, il Titolare ha la facoltà di designare persone fisiche, che operano sotto la propria autorità, attribuendo loro specifici compiti e funzioni connesse al trattamento di dati personali.

Il Responsabile (interno) è tenuto a coadiuvare il Titolare nella definizione delle finalità, delle modalità del trattamento e dei mezzi per garantire l'osservanza della normativa europea e nazionale vigente.

Autorizzati al trattamento (Incaricati)

Il Regolamento non prevede espressamente la figura dell'incaricato, ma l'art. 29 chiarisce che i soggetti che, sotto l'autorità del Titolare o del Responsabile, effettuano materialmente operazioni di trattamento, devono essere autorizzati e devono operare sulla base di apposite istruzioni e/o con diversi livelli di delega da parte del Titolare.

Quindi sono da considerarsi Autorizzati al trattamento tutti coloro che compiono operazioni di trattamento dati personali, sia su supporti cartacei che informatici, per quanto di rispettiva competenza, afferenti ordinariamente presso la struttura di riferimento o che pongano in essere con la struttura rapporti di servizio, collaborazione, studio e ricerca (personale t.a., docenti, ricercatori, assegnisti, borsisti, collaboratori, ecc.)

I responsabili del trattamento, contestualmente alla comunicazione di una nuova assegnazione di personale alla struttura, dovranno provvedere alla definizione dei trattamenti a lui autorizzati e fornirgli specifiche istruzioni.

PRINCIPI GENERALI

Il Regolamento codifica i principi generali del trattamento, i quali hanno una valenza che copre ogni angolazione della disciplina e devono essere rispettati in ogni fase del trattamento dei dati.

L'art. 5 del GDPR afferma che ogni trattamento di dati personali deve avvenire nel rispetto dei seguenti principi:

- **liceità, correttezza e trasparenza** del trattamento, nei confronti dell'interessato;
- **limitazione della finalità** del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- **minimizzazione dei dati**, ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- **esattezza e aggiornamento dei dati**, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- **limitazione della conservazione** per la quale è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- **integrità e riservatezza,** per le quali occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento. Il Titolare è tenuto a mettere in atto misure tecniche e organizzative adeguate a prevenire trattamenti non autorizzati o illeciti o perdita, distruzione o danno accidentale e deve essere in grado di dimostrare il rispetto di tali principi.

Liceità del trattamento

Il Regolamento, all'art. 6, dispone che ogni trattamento deve trovare fondamento in un'idonea base giuridica, perché possa essere lecito.

Il Titolare del trattamento ha l'obbligo di valutare quale sia la base giuridica più idonea rispetto al trattamento che intende porre in essere (finalità). Deve quindi rispettare le condizioni previste dal GDPR riguardo ciascuna delle basi indicate nell'art. 6 ed essere sempre in grado di dimostrare la correttezza della scelta fatta.

I fondamenti di liceità del trattamento di dati personali sono: il consenso, l'adempimento di obblighi contrattuali, gli interessi vitali della persona interessata o di terzi, gli obblighi di legge cui è soggetto il Titolare, l'interesse pubblico o l'esercizio di pubblici poteri, l'interesse legittimo prevalente del Titolare o di terzi cui i dati vengono comunicati.

Il Codice privacy italiano, all'art 2-*ter*, specifica che la base giuridica per le attività di interesse pubblico e l'esercizio di pubblici poteri, deve essere esclusivamente una norma di legge o, nei casi previsti dalla legge, o di regolamento.

Il Garante può inoltre prescrivere misure a garanzia dell'interessato per i trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati.

Consenso dell'interessato

Il consenso dell'interessato è un delle basi giuridiche del trattamento. In base al GDPR (art. 4), il consenso è "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano siano oggetto di trattamento".

Nei trattamenti in cui la base giuridica è rappresentata da interesse pubblico o esercizio di pubblici poteri, qualora il trattamento sia previsto per legge e rientri nelle finalità istituzionali dell'Ente, il consenso non è dovuto.

Quando il trattamento si fonda sul consenso dell'interessato, l'art. 7 del GDPR prescrive che il Titolare deve sempre essere in grado di dimostrare che l'interessato ha prestato il proprio consenso, che è valido se

all'interessato è stata resa l'informativa sul trattamento dei dati personali e se è stato espresso liberamente, in modo inequivocabile e specificamente con riguardo a ciascuna finalità.

Il consenso è revocabile e deve essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato.

ADEMPIMENTI FORMALI

Registro dei trattamenti

Il Titolare e il Responsabile (esterno) del trattamento sono obbligati alla tenuta di Registri delle attività di trattamento.

Il Registro è un documento che deve contenere una serie di informazioni, specificate all'art.30 del GDPR, relative al Titolare e alle operazioni di trattamento da lui svolte e quindi costituisce lo strumento idoneo a fornire la rappresentazione, sempre aggiornata, dell'organizzazione e dei trattamenti svolti.

Il Registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta del Garante.

La tenuta del Registro rappresenta uno dei principali elementi di *accountability* del Titolare, finalizzato anche all'analisi del rischio e ad una corretta pianificazione dei trattamenti.

Valutazione d'impatto sulla protezione dei dati

Nei casi richiesti dall'art. 35 del GDPR, o qualora un trattamento presenti un rischio elevato, il Titolare, prima di procedere al trattamento stesso, deve effettuare una valutazione dell'impatto sulla protezione dei dati personali.

DIRITTI DEGLI INTERESSATI

L'interessato ha il diritto di essere informato preventivamente dal Titolare, perché possa essere consapevole dello scopo legittimo per il quale i dati sono stati forniti e per metterlo nelle condizioni di esercitare i propri diritti

Il Regolamento introduce una serie di diritti, qui sotto in parte elencati, che l'interessato può fare valere attraverso una richiesta al Titolare.

Diritto all'informazione (Informativa all'interessato)

Quando un Titolare effettua un trattamento, deve fornire all'Interessato le informazioni, elencate negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento, in modo conciso, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro.

L'Informativa deve esser resa all'interessato all'atto della raccolta dei dati e prima di effettuare il trattamento. Il documento deve contenere, i dati del Titolare del trattamento, i dati di contatto del RPD (Responsabile della Protezione dei Dati), la base giuridica del trattamento, se i dati sono soggetti ad essere trasferiti verso Paesi terzi; deve, inoltre, elencare i diritti dell'interessato e le modalità per poterli esercitare.

Il Regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente"; in particolare, il Titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione nonché le modalità per presentare un reclamo all'autorità di controllo.

L'informativa deve specificare se i trattamenti comportano processi decisionali automatizzati, fra cui la profilazione.

Diritto di accesso

Il diritto di accesso prevede che l'interessato possa chiedere e ricevere dal Titolare una copia dei dati personali oggetto di trattamento, con l'indicazione del periodo di conservazione previsto e delle garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

Diritto alla cancellazione (diritto all'oblio)

Qualora il Titolare riceva da parte dell'Interessato una domanda di cancellazione dei dati che lo riguardano, deve procedere ad evadere la richiesta senza ingiustificato ritardo in tutti i casi (previsti dall'art.17) in cui in cui i dati personali non siano più necessari rispetto alle finalità per cui erano stati originariamente trattati oppure siano stati trattati illecitamente oppure l'interessato revochi il consenso o si opponga al loro trattamento oppure la cancellazione costituisca un obbligo giuridico imposto dal diritto dell'UE o degli Stati membri.

Il diritto alla cancellazione comporta l'obbligo per i Titolari, se hanno reso pubblici i dati personali dell'Interessato pubblicandoli su un sito web, di informare della richiesta di cancellazione altri Titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".

Diritto di rettifica di dati personali inesatti o incompleti

Il diritto di rettifica consente all'Interessato di ottenere dal Titolare del trattamento la rettifica e/o l'integrazione dei dati personali che lo riguardano senza ingiustificato ritardo.

Diritto alla limitazione del trattamento

Il diritto di limitazione del trattamento, previsto all'articolo 18, è uno dei diritti esercitabili dall'interessato nei confronti del Titolare, al quale viene richiesto che, il trattamento dei dati personali sia limitato a quanto necessario ai fini della conservazione.

Il GDPR definisce la limitazione di trattamento: "il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro".

Negli archivi automatizzati consiste quindi nell'attivare una funzionalità informatica, che permetta di "contrassegnare" i dati personali memorizzati, che non possono essere sottoposti a ulteriori trattamenti e non possano essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

Il regolamento, al Cons. 67, suggerisce alcune delle modalità attraverso le quali è possibile limitare il trattamento dei dati personali:

- trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento;
- rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web.

Diritto di opposizione

L'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano (art. 21).

L'Interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida significatamene sulla sua persona.

Il Titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'Interessato, adottando ogni idonea misura tecnica e organizzativa e il termine per la risposta all'Interessato è un mese, estendibile fino a tre mesi in casi di particolare complessità; il Titolare deve comunque dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego.

All'art. 2-undiecies del d.lgs. 196/2003, si prevede che i diritti dell'interessato possano essere ritardati, limitati o esclusi con comunicazione motivata se dal loro esercizio deriva un pregiudizio concreto agli interessi tutelati in materia di riciclaggio, di sostegno alle vittime di richieste estorsive, di attività delle commissioni parlamentari di inchiesta, di politica monetaria, di investigazioni difensive, di tutela del dipendente che segnala illeciti.

SICUREZZA

Sicurezza

Il Titolare e il Responsabile del trattamento sono obbligati, dall'articolo 32 del GDPR, ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato alla valutazione del rischio del trattamento, con l'obiettivo di evitare distruzioni accidentali o illecite, perdite, modifiche, rivelazioni, accessi non autorizzati (*data breach*).

L'adeguato livello di sicurezza delle misure progettate e realizzate deve essere assicurato, attraverso un bilanciamento tra i costi di attuazione, lo stato dell'arte e la natura dei dati che devono essere protetti ed i rischi che presentano i trattamenti.

Fra tali misure sono menzionate: la pseudonimizzazione e la cifratura dei dati; quelle per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; quelle atte a garantire il tempestivo ripristino della disponibilità dei dati; le procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

L'art. 2-septies (d.lgs. 101/2018), in presenza di trattamenti di dati genetici, biometrici e relativi allo stato di salute, richiede inoltre la conformità alle misure di garanzia disposte dal Garante.

Violazione dei dati personali (*data breach*)

La violazione di sicurezza comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, in modo accidentale o illecito.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Nei casi di c.d. *data breach*, l'articolo 33 del GDPR prevede alcuni adempimenti fra cui: la comunicazione all'interessato e la notifica, entro 72 ore, al Garante della protezione dei dati personali

Il Titolare deve documentare le violazioni di dati personali subite, anche se non notificate all'Autorità di controllo e/o non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Principio di responsabilizzazione (*accountability*)

Il GDPR evidenzia il principio della "responsabilizzazione" (c.d. *accountability*) dei Titolari e dei Responsabili del trattamento che consiste nell'assumere comportamenti proattivi, tali da dimostrare la concreta adozione di adeguate misure di carattere preventivo finalizzate ad assicurare l´applicazione del

Regolamento e la tutela dei diritti e delle libertà dei soggetti interessati e delle persone. Ciò implica, tra l'altro, che l'intervento del Garante sarà principalmente "ex post", collocandosi successivamente alle determinazioni che il Titolare assume con autonomia.

Protezione per impostazione predefinita (*privacy by design e privacy by default*)

Il Titolare del trattamento è obbligato a mettere in atto misure di sicurezza preventive adeguate, prestabilendo "a monte" – quindi già dal momento in cui vengono determinati i mezzi del trattamento, ma anche durante il trattamento stesso – tutte le cautele necessarie a soddisfare i requisiti del Regolamento, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Le misure volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, devono garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento.

ILLECITI E SANZIONI

Illeciti penali

Gli artt. da 167 a 172 del D.Lgs. 196/2003 prevedono diverse tipologie di reati che conseguono ad ipotesi di trattamenti di dati effettuati in violazione delle disposizioni di legge e in presenza dell'intenzione di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato. Le ipotesi di reato riguardano, tra l'altro, il traffico telefonico, le comunicazioni indesiderate, la diffusione o l'acquisizione illegittima di un archivio, l'inosservanza dei provvedimenti adottati dal Garante e comportano pene di reclusione fino a sei anni.

Sanzioni

Il GDPR (artt. 83 e 84) prevede sanzioni amministrative pecuniarie, fino a euro 10.000,00 o al 2% del fatturato per alcune tipologie di violazioni e fino a euro 20.000,00 o al 4% del fatturato per altre tipologie di violazioni.

L'art. 166 del d.lgs. 196/2003 stabilisce le violazioni soggette alla prima tipologia di sanzioni e quelle soggette alla seconda tipologia e indica, quale organo competente ad irrogare le sanzioni, il Garante della protezione dei dati personali. Il Garante definirà con un proprio regolamento le modalità del procedimento per l'adozione dei provvedimenti e delle sanzioni.

SPECIFICI TRATTAMENTI

Il nuovo Codice *privacy*, adeguato dal d.lgs. 101/2018, detta disposizioni in materia di trattamento dei dati personali relativi a specifici settori, fra cui**:**

Trattamento dei dati relativi agli studenti

Le istituzioni che operano nel sistema dell'istruzione, comprese le università, possono, su richiesta degli interessati, comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali pertinenti, con esclusione dei dati particolari e giudiziari come definiti agli articoli 9 e 10 del GDPR. La norma ribadisce che i dati possono essere trattati solo per le finalità indicate nelle informative rese agli interessati (art. 96).

Trattamenti di dati a fini di ricerca

Le università, con autonome determinazioni, possono comunicare e diffondere dati relativi ad attività di studio e di ricerca a laureati, dottori di ricerca, ricercatori, docenti, esperti e studiosi per attività di studio e di ricerca, con esclusione dei dati particolari e giudiziari.

Restano fermi i diritti dell'interessato di rettifica, cancellazione, limitazione e opposizione disposti dal GDPR. In quest'ambito il Garante promuove l'adozione di apposite regole deontologiche (artt. da 100 a 110-bis).

Il Garante per la protezione dei dati, ha adottato in data 19 dicembre 2018 le "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101" [doc. web n. 9069637]

Inoltre per il trattamento di categorie particolari di dati da parte di ricercatori, a seguito di quanto fissato dall'art. 21 del d.lgs. 2018/101 in attuazione delle disposizioni del Regolamento europeo, il Garante ha adottato nel "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati" [doc. web n. 9124510], le "Prescrizioni relative al trattamento dei dati genetici" e le "Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica " Tali disposizioni sono prescrittive e pertanto i ricercatori sono obbligati ad attenersi.

Curriculum

Il consenso al trattamento dei dati personali non è dovuto se i curriculum vengono spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro.

Il Titolare può fornire le informative al momento del primo contatto utile, successivo all'invio del curriculum medesimo (art. 111-bis).

Accesso a documenti amministrativi e accesso civico

Per quanto riguarda i trattamenti in ambito pubblico, e in particolare con riferimento ai rapporti tra protezione dei dati personali e accesso ai documenti amministrativi, la norma (art. 59 punto 1), rinvia alla disciplina prevista dalla legge n. 241/1990, mentre al punto 1-bis prevede che i presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restino disciplinati dal d.lgs. 33/2013.

Se l'accesso riguarda i dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, l'art. 60 lo consente solo se la situazione giuridicamente rilevante che si intende tutelare, con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Trattamento di dati riguardanti i datori di lavoro

L'art. 113 del Codice ribadisce che resta fermo quanto stabilito dall'art. 8 della legge n. 300/1970 e dall'art. 10 del d.lgs. n. 276/2003, i quali specificano il divieto del datore di lavoro di effettuare indagini sulle opinioni politiche dei lavoratori e su altri elementi che non siano attinenti alle attitudini professionali e all'inserimento lavorativo. L'art. 114, poi, conferma le disposizioni della legge n. 300/1970 sul controllo a distanza del lavoratore.

Il Garante per la protezione dei dati, a seguito di quanto fissato dall'art. 21 del d.lgs. 2018/101 in attuazione delle disposizioni del Regolamento europeo. ha adottato nel Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, le "Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016"), rivolte anche a datori di lavoro pubblici;

RIFERIMENTI NORMATIVI E APPROFONDIMENTI:

Riferimenti normativi:

Regolamento (UE) 2016/679 “Relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati” (versione italiana)
https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018.pdf/1bd9bde0-d074-4ca8-b37d-82a3478fd5d3?version=1.9

Decreto legislativo 101/2018 “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679”
https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true

D.Lgs. 2003/196 Codice in materia di protezione dei dati personali (atto vigente)
http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig=2023-02-10

Approfondimenti:

Autorità Garante per la protezione dei dati
https://www.garanteprivacy.it/

Comitato europeo per la protezione dei dati (EDPB)
https://edpb.europa.eu/edpb_it

Linee guida EDPB
Guidelines | European Data Protection Board (europa.eu)