



CAMERA DI
COMMERCIO
MILANO
MONZABRIANZA
LODI



VADEMECUM SUL TRATTAMENTO DEI DATI PERSONALI ALLA LUCE DEL GDPR

A cura dello Studio Legale Lisi



VADEMECUM SUL TRATTAMENTO DEI DATI PERSONALI ALLA LUCE DEL GDPR

INDICE

PREMESSA	8
I) PRINCIPI E BASI GIURIDICHE DEL TRATTAMENTO, SOGGETTI E DIRITTI DEGLI INTERESSATI	10
1. Le basi giuridiche del trattamento	11
2. I soggetti del trattamento	12
3. I diritti degli interessati	15
3.1. Il diritto di accesso ai propri dati (art. 15 GDPR)	15
3.2. Diritto di rettifica (art. 16 GDPR)	16
3.3. Diritto alla cancellazione (art. 17 GDPR)	16
3.4. Diritto di limitazione di trattamento (art. 18 GDPR)	17
3.5. Diritto alla portabilità dei dati (art. 20 GDPR)	18
3.6. Diritto di opposizione (art. 21 GDPR)	18
3.7. Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (art. 22 GDPR)	19
II) MARKETING E PROFILAZIONE	20
1. Come distinguere il marketing dalla profilazione	21
2. Il consenso nelle attività di marketing diretto (“soft spam”)	21
3. Newsletter. Adempimenti per una corretta gestione	22
4. Informativa multistrato per i processi decisionali automatizzati (compresa la profilazione)	23
5. Acquisizione del consenso in caso di profilazione di utenti non autenticati	23

III) ANALISI DEL SITO WEB AZIENDALE	25
1. Cosa sono e a cosa servono i cookie	26
2. Tipologie di cookie	26
2.1 Cookie tecnici	26
2.2 Cookie di profilazione	27
3. Cookie e consenso	27
4. Informative e manifestazione del consenso	28
5. Contenuto della Cookie policy	30
IV) IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO	31
1. Natura e funzioni del Registro delle attività di trattamento	32
2. Obbligo di tenuta del Registro delle attività di trattamento	32
3. Contenuti del Registro delle attività di trattamento	34
4. Modalità di conservazione e aggiornamento del Registro delle attività di trattamento	35
5. Il Registro del responsabile del trattamento	36
V) ACCOUNTABILITY PRIVACY BY DESIGN E BY DEFAULT	38
1. Il concetto di accountability	39
2. Soggetti tenuti al rispetto del principio di accountability	39
3. I principali adempimenti richiesti dal principio di accountability	40
4. Privacy by design e by default	40
VI) LE INFORMATIVE PRIVACY	42
1. Perché è importante fornire le informative privacy	43
2. Dati raccolti presso l'interessato (art. 13, par. 1 e 2): quali informazioni fornire	43
3. Dati raccolti presso l'interessato: trattamento per finalità diversa	45
4. Dati raccolti presso soggetto diverso dall'interessato (art. 14)	46
VII) DPO: RUOLO, COMPITI E FUNZIONI	47
1. Quali sono i compiti che il DPO è chiamato a svolgere	48
2. Quali caratteristiche deve avere il DPO	49
3. Posizione del DPO all'interno dell'organizzazione	50
3.1. DPO e conflitto di interessi	50

3.2. Possibili casi di conflitto di interessi	51
VIII) IL DATA BREACH	52
1. Cosa si intende per data breach	53
2. La notifica di un data breach all'Autorità di controllo	53
3. Contenuto minimo della notifica al Garante	54
4. La comunicazione all'interessato	55
4.1. Requisiti della comunicazione all'interessato	55
4.2. Quando non è richiesta la comunicazione all'interessato	55
5. Valutazione del rischio conseguente a un data breach	56
IX) GLI AMMINISTRATORI DI SISTEMA	58
1. Qual è il ruolo dell'amministratore di sistema?	59
2. Misure da adottare nella designazione e gestione degli amministratori di sistema	59
3. Verifica delle attività degli amministratori di sistema	60
4. Come qualificare l'amministratore di sistema alla luce del GDPR	61
5. Sicurezza del trattamento operato dall'amministratore di sistema	62
X) CONTROLLO DEI LAVORATORI E VIDEOSORVEGLIANZA	63
1. A quali condizioni il datore di lavoro può trattare i dati dei lavoratori	64
2. Presupposti per il controllo dei lavoratori a distanza	64
3. La navigazione in internet del lavoratore	66
4. L'uso della posta elettronica da parte del lavoratore	67
5. Legittimità dei controlli basati su tecniche di riconoscimento biometrico	68
XI) ULTERIORI APPROFONDIMENTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI	70
1. Nell'ambito delle attività di marketing diretto, in che modo il titolare dimostra che non è necessario il consenso degli interessati?	71
2. Le società o gli studi di consulenza regolatoria hanno l'obbligo di nominare un DPO e della tenuta del Registro dei trattamenti?	71
3. È obbligatorio nominare individualmente le persone autorizzate al trattamento?	72

4. Nell'ambito delle attività svolte in qualità di CTU (Consulente Tecnico d'Ufficio), è necessario rendere l'informativa alle parti?	72
5. Gli obblighi assolti ai sensi del GDPR per attività svolte in qualità di titolare del trattamento a favore di un cliente, in virtù di un contratto di consulenza, restano fermi anche in caso di incarico di CTU assegnato dall'autorità giudiziaria, in un procedimento in cui è parte lo stesso cliente?	74
6. Cosa succede se un cliente chiede espressamente l'anonimato?	74
7. Alcuni esempi di legittimi interessi quali base giuridica del trattamento	74

PRESENTAZIONE

In un'epoca come quella attuale – segnata da un incessante avanzamento tecnologico e dalla conseguente possibilità di incrociare ed elaborare quantità di dati finora inimmaginabili – emerge in modo del tutto evidente la necessità di tutelare le informazioni personali, garantendo a chiunque fruisca dei servizi della società dell'informazione di poter rimanere nel loro pieno controllo.

In questa prospettiva, il Regolamento (UE) 2016/679 ha segnato un importante traguardo, delineando un quadro di riferimento uniforme a livello europeo per la gestione dei dati personali, con l'obiettivo di assicurare un elevato livello di protezione dei diritti e delle libertà delle persone fisiche attraverso un insieme di norme concernenti il corretto trattamento di tali dati.

L'adeguamento al nuovo Regolamento ha innegabilmente comportato importanti sforzi per le imprese che si sono ritrovate ad esplorare territori per certi versi nuovi, affrontando sfide significative per ciò che concerne la corretta gestione dei dati personali.

Conscia di queste sfide – anche quale soggetto coinvolto in prima linea nelle nuove prospettive tracciate dal Regolamento – nel 2019 la Camera di Commercio di Milano Monza Brianza Lodi ha voluto accompagnare le proprie imprese in un percorso formativo teso a fornire le consapevolezze operative fondamentali per poter affrontare e gestire questo cambiamento.

Il lavoro che segue rappresenta la conclusione di questo percorso e ne sintetizza lo spirito e i contenuti: si tratta, infatti, di una guida operativa che ha lo scopo di illustrare i tratti salienti della disciplina, mettendo l'accento sui potenziali problemi di natura applicativa che le imprese – e in generale tutti coloro che si trovino a dover mettere in pratica il Regolamento – possono incontrare, ma fornendo anche spunti pratici per agevolarne il rispetto.

L'auspicio è che i frutti di questo percorso costituiscano un patrimonio informativo utile per tutte le imprese che, cimentandosi nella concreta applicazione del Regolamento, possano contribuire ad una effettiva e non troppo onerosa tutela dei dati personali a vantaggio di tutti noi consumatori.

Carlo Sangalli

Presidente Camera di Commercio di Milano Monza Brianza Lodi

PREMESSA

Con il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (General Data Protection Regulation, “GDPR”), divenuto direttamente applicabile in tutti gli ordinamenti degli Stati membri dell’Unione europea dal 25 maggio 2018, è stata abrogata la Direttiva 95/46/CE, andando a disegnare un nuovo sistema di protezione dei dati personali che mette al centro la persona, offrendo al contempo alle organizzazioni, titolari o responsabili del trattamento, una bussola per orientarsi tra i rischi che i trattamenti comportano e adottare le misure necessarie sulla base del principio di responsabilizzazione (accountability).

L’intento del GDPR è duplice: stabilire norme relative alla protezione delle persone fisiche (cc.dd. interessati) con riguardo al trattamento dei dati personali, senza pregiudicare la libera circolazione dei dati e delle informazioni, anche personali, cruciale per lo sviluppo dell’economia digitale nell’ambito del mercato interno dell’Unione europea.

In via preliminare, occorre chiarire che un dato è da considerarsi “personale” se contiene un’informazione riferibile a una persona fisica determinata o determinabile. Il trattamento di dati personali riferiti a persone giuridiche, quindi, non rientra nel campo di applicazione del GDPR.

È utile specificare, poi, che il GDPR si applica non soltanto a tutti i titolari e responsabili del trattamento che abbiano sede in un Paese membro dell’Unione europea, ma anche a tutti i soggetti, le organizzazioni e i servizi che, ovunque stabiliti, trattino dati di interessati che si trovano nell’Unione europea.

Inoltre, è opportuno precisare che qualora una persona fisica tratti dati personali relativi ad altri soggetti nell’ambito di attività a carattere esclusivamente personale o domestico, non si rientra nell’ambito di applicazione del GDPR (art. 2, par. 2, lett. c), GDPR) e pertanto non si è soggetti all’obbligo di rispettarne le relative norme. Ad esempio, la gestione della propria corrispondenza privata, la tenuta di un diario o di un blog ove siano presenti dati personali relativi alla partecipazione a eventi con colleghi o a incontri con partner professionali, sono certamente estranei all’applicazione del GDPR, anche qualora tali trattamenti siano svolti mediante l’uso di social network o comunque online, a patto tuttavia che il trattamento di tali dati avvenga per finalità strettamente personali.

Non sempre, però, è agevole distinguere le attività a carattere personale da altre che non lo sono. In effetti, occorre considerare che le attività personali di trattamento di dati di terzi interessati che comunque presentino aspetti

professionali o commerciali possono comportare la piena applicazione del GDPR.

Proprio nell'ottica di fornire chiarimenti ai dubbi che sorgono in relazione alle applicazioni concrete del GDPR in un contesto commerciale o aziendale, il presente vademecum si propone come uno strumento agile e di pronta consultazione in favore di società e studi professionali che trattano dati personali nel contesto della propria organizzazione, finalizzato a descrivere con chiarezza gli aspetti più importanti della disciplina posta a tutela dei dati personali, con esempi concreti a corredo degli aspetti teorici.

Il presente Vademecum, redatto dagli avvocati Mario Montano e Sarah Ungaro, sotto la mia supervisione, costituisce il percorso finale di una serie di seminari sviluppati in favore della CCIAA di Milano Monza Brianza Lodi e, nella sua parte finale, si è cercato di rispondere ai vari quesiti posti durante i vivaci confronti emersi con gli imprenditori.

Si tratta comunque di un supporto sintetico ed essenziale e si consiglia sempre e in ogni caso di approfondire ogni aspetto trattato e di aggiornarsi periodicamente attraverso il sito web dell'Autorità Garante per la protezione dei dati personali (<https://www.garanteprivacy.it/>).

Buona lettura.

Milano, 3 dicembre 2019

Avv. Andrea Lisi

(Studio Legale Lisi)

I *Principi e basi giuridiche del trattamento, soggetti e diritti degli interessati*

1. LE BASI GIURIDICHE DEL TRATTAMENTO

Com'è noto, il Regolamento 2016/679 UE è direttamente applicabile in tutti gli Stati membri dell'Unione europea, tuttavia, l'Italia ha dovuto comunque adottare il D.Lgs. 101/2018 per adeguare le norme contenute nel D.Lgs. 196/2003 alle nuove regole dettate dal GDPR.

Il vecchio impianto normativo si fondava sulla centralità del consenso dell'interessato, a garanzia della legittimità dei trattamenti effettuati dal titolare, mentre il GDPR ha mutato tale assetto, prevedendo il consenso dell'interessato solo come uno dei casi che rendono leciti i nostri trattamenti. Tra le basi giuridiche del trattamento, infatti, l'art.6 GDPR comprende sì il consenso dell'interessato, ma accanto ad altre numerose ipotesi:

1. La necessità di dare esecuzione a un contratto di cui l'interessato è parte o a misure precontrattuali adottate su richiesta dello stesso;
2. L'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento, come ad esempio il trattamento dei dati dei dipendenti compiuto dal datore di lavoro per motivi di previdenza sociale e fiscalità;
3. La salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, come il caso di epidemie o emergenze umanitarie;
4. L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (es., trattamenti di dati personali svolti per finalità inerenti all'espletamento di attività istituzionali e statutarie di istituti di istruzione, anche paritari; Ordini e Collegi professionali; strutture cliniche o sociosanitarie, anche private; Centri di Assistenza Fiscale (CAF) e Centri Autorizzati di Assistenza Fiscale (CAAF), etc.);
5. Il perseguimento di un interesse legittimo² del titolare del trattamento o di terzi. Così, il considerando 47 del GDPR annovera fra gli interessi legittimi la trasmissione di dati personali all'interno di uno stesso gruppo imprenditoriale a fini amministrativi interni (es. gestione del personale), la prevenzione delle frodi o l'attività di marketing diretto, volta, cioè, a comunicare direttamente con clienti specifici, ad esempio mediante l'uso di singole e-mail. L'art. 130, comma 4, D.lgs. 196/2003, come si vedrà meglio più avanti, disciplina i casi in cui è possibile utilizzare il c.d. soft spam senza richiedere il consenso dell'interessato.

2. Purché il legittimo interesse sia sufficientemente articolato da permettere una valutazione di prevalenza (da effettuare caso per caso) rispetto all'interesse o ai diritti fondamentali dell'interessato, soprattutto nel caso in cui quest'ultimo sia un minore, e lo stesso possa dirsi reale e attuale, cioè corrisponda a un beneficio concreto e atteso in un futuro prossimo.

Giova ricordare che il Gruppo WP29, il Gruppo di Lavoro previsto dall'art. 29 Direttiva UE 95/46, ora Comitato Europeo per la Protezione dei Dati (EDPB), ha osservato che se il titolare del trattamento sceglie il consenso quale propria base giuridica per legittimare un trattamento di dati personali, lo stesso titolare non può basare successivamente il trattamento su una diversa base giuridica, ricorrendo, ad esempio, all'interesse legittimo in caso di problemi di validità del consenso. Ciò in quanto il titolare ha l'obbligo di comunicare all'interessato il presupposto di liceità del trattamento al momento della raccolta dei dati personali³.

2. I SOGGETTI DEL TRATTAMENTO

Diversi sono gli attori del trattamento dei dati personali: l'interessato, il titolare del trattamento, il responsabile del trattamento, l'eventuale rappresentante del titolare o del responsabile, il responsabile per la protezione dei dati (RPD) o data protection officer (DPO), l'autorizzato/designato, i destinatari.

Il **titolare** è definito dal GDPR (art. 4) come quel soggetto che determina le finalità e i mezzi del trattamento di dati personali. Può essere una persona fisica o giuridica, un'autorità pubblica, un servizio o un altro organismo.

Se due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, sono da considerarsi **contitolari** del trattamento (art. 26, GDPR).

I contitolari determineranno in un accordo specifico le rispettive responsabilità per il rispetto degli obblighi previsti dal regolamento.

Il **responsabile del trattamento**, invece, è la persona fisica o giuridica che tratta i dati per conto del titolare del trattamento, seguendo istruzioni precise, contenute in un contratto o altro atto giuridico vincolante. Sebbene il titolare sia tenuto a esercitare sempre un controllo sul trattamento, il responsabile del trattamento, come il titolare, ha degli obblighi specifici che spesso si affiancano a quelli del titolare stesso. Deve tenere un Registro di tutte le categorie di attività relative al trattamento (art. 30 GDPR), mettere in atto misure tecniche e organizzative adeguate per garantire la sicurezza del trattamento (art. 32, GDPR), designare, in determinate situazioni, un responsabile della protezione dei dati (art. 37, GDPR).

La maggiore responsabilizzazione del titolare e del responsabile del

3. Per approfondimenti si veda https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

trattamento⁴, unita alla crescente complessità e ai rischi per i diritti e le libertà delle persone fisiche derivante dal trattamento dei dati personali nell'attuale contesto, ha indotto il legislatore europeo a introdurre nella disciplina del GDPR un'importante figura, alla quale si richiede il possesso di requisiti di elevata professionalità e competenza, il DPO o RPD. Il **responsabile per la protezione dei dati** (RPD), in effetti, ha il compito di fornire un supporto consulenziale (al titolare o al responsabile che lo ha nominato) sul rispetto delle norme in materia di protezione dei dati, agendo al contempo da punto di contatto con l'autorità di controllo.

L'art. 37, GDPR, prevede l'obbligo di nominare un RPD in tre casi:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- se le attività principali del titolare del trattamento o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- se le attività principali del titolare o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 GDPR o di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR.

L'RPD è in genere un professionista esterno all'organizzazione, che ricopre tale ruolo in base a un contratto di servizi, ma può anche essere un dipendente del titolare o del responsabile del trattamento (art. 37, p. 6, GDPR). Le organizzazioni più complesse, come ad esempio i gruppi imprenditoriali, possono nominare un solo RPD, purché sia facilmente raggiungibile da ciascuno stabilimento (art. 37, p. 2, GDPR)⁵. Lo stesso potranno fare più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione (art. 37, p. 3, GDPR).

L'articolo 39 del GDPR specifica i compiti e le funzioni degli RPD. Questi includono gli obblighi di informare e fornire consulenza al titolare (o al responsabile) che l'ha nominato, nonché al personale dello stesso che esegue le attività di trattamento (autorizzati al trattamento), in merito ai loro obblighi derivanti dalla legislazione, sorvegliare l'osservanza delle norme dell'Unione

4. Titolare e responsabile secondo l'art. 82, paragrafo 1, rispondono congiuntamente nei confronti di un interessato che abbia subito un danno a causa di un trattamento da essi svolto in violazione del GDPR. Occorre precisare, però, che secondo il secondo paragrafo dello stesso articolo, mentre la responsabilità del titolare verso gli interessati è piena, quella del responsabile dipende dalle istruzioni conferite dal titolare e dagli obblighi direttamente a esso attribuiti dal GDPR.

5. Sul punto si vedano anche le Linee guida sul Responsabili della protezione dei dati (RPD) emanate dal WP 29 (adottate il 13 dicembre 2016, 16/EN – WP 243).

europea o dell'ordinamento nazionale sulla protezione dei dati attraverso attività di controllo e la formazione del personale che partecipa ai trattamenti. Gli RPD devono, inoltre, - come già specificato - cooperare con l'autorità di controllo e fungere da punto di contatto per quest'ultima per questioni connesse al trattamento dei dati come, per esempio, un'eventuale violazione dei dati personali.

Per assicurare l'indipendenza dell'RPD, il GDPR stabilisce alcune garanzie di base. I titolari del trattamento e i responsabili del trattamento, infatti, devono assicurare che, nell'esecuzione dei compiti relativi alla protezione dei dati, gli RPD non ricevano alcuna istruzione, incluso da eventuali superiori gerarchici. Inoltre, essi non possono essere rimossi o penalizzati in alcun modo per l'adempimento dei compiti propri di RPD.

Per quanto attiene, diversamente, allo svolgimento dei trattamenti per conto del titolare o del responsabile del trattamento, questi ultimi possono affidare specifici compiti e funzioni a figure interne alla loro organizzazione, che operano sotto la loro responsabilità.

A tal fine, il GDPR impone al titolare o al responsabile del trattamento di individuare quei soggetti all'interno dell'organizzazione - c.d. **autorizzati**⁶ - che hanno il compito di trattare tali dati, e di fornire agli stessi specifiche istruzioni sul trattamento, specificando che gli stessi agiscono sotto la diretta autorità del titolare o del responsabile (art. 29 GDPR).

Sulla scorta di questa previsione, e dovendo salvaguardare i compiti e le funzioni già assegnati all'interno delle organizzazioni sulla base del sistema previgente e non più compatibili con il GDPR, il legislatore italiano ha ritenuto opportuno introdurre, con l'art. 2-quaterdecies, D.Lgs. 196/2003⁷, la figura del **designato**, persona fisica individuata dal titolare (o dal responsabile del trattamento) nell'ambito del proprio assetto organizzativo, la quale opera sotto la sua autorità e alla quale sono attribuiti specifici compiti e funzioni, tra cui anche quelli relativi all'organizzazione e al coordinamento delle attività di trattamento di cui sono incaricati gli altri soggetti autorizzati.

I dati personali, una volta raccolti dal titolare, possono essere comunicati ad altri soggetti, ad esempio, i contitolari, i responsabili del trattamento, gli autorizzati, i soggetti esterni che ex lege devono riceverli ecc. Sono

⁶ *Ai sensi del precedente codice in materia di protezione dei dati personali (D.Lgs. 196/2003), era possibile assegnare delle funzioni a figure interne, definite, a seconda dei casi, responsabili del trattamento (art. 29) o incaricati (art. 30).*

⁷ *Ai sensi del precedente codice in materia di protezione dei dati personali (D.Lgs. 196/2003), era possibile assegnare delle funzioni a figure interne, definite, a seconda dei casi, responsabili del trattamento (art. 29) o incaricati (art. 30).*

tutti **destinatari**, appartengano o meno all'organizzazione del titolare del trattamento. In effetti, l'art. 4, par. 9, GDPR, definisce "destinatario" «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi». È **terzo**, quindi, «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **non** sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile». In tal senso, ad esempio, l'azienda che eroga i ticket dei buoni pasto, a cui l'organizzazione comunica i dati dei propri dipendenti, sarà da considerarsi quale soggetto terzo.

3. I DIRITTI DEGLI INTERESSATI

La protezione dei dati personali degli interessati è assicurata dal riconoscimento di una serie di diritti, elencati analiticamente agli artt. 15-22 GDPR.

Come si chiarirà meglio più avanti, l'interessato è messo nelle condizioni di esercitare i propri diritti attraverso le informazioni che il titolare è tenuto a fornirgli nel momento in cui raccoglie i suoi dati personali (art. 13 GDPR) o lo fa mediante altre fonti, e non direttamente presso l'interessato (art. 14 GDPR).

3.1 I DIRITTI DI ACCESSO AI PROPRI DATI (ART. 15 GDPR)

Prodromico all'esercizio di tutti gli altri diritti, il diritto di accesso ai propri dati personali è riconosciuto all'interessato all'art. 15 GDPR. Il titolare del trattamento dovrà fornire all'interessato una copia dei dati personali oggetto di trattamento, in forma intelligibile, cioè con modalità tali da facilitare la comprensione delle informazioni fornite.

Nello specifico, l'interessato ha il diritto di sapere se un trattamento dei propri dati personali è in corso e di accedere alle seguenti informazioni:

- finalità del trattamento;
- categorie dei dati in questione;
- destinatari o categorie di destinatari a cui i dati sono comunicati;
- periodo di conservazione dei dati personali previsto oppure, se non è possibile, criteri utilizzati per determinare tale periodo;
- esistenza del diritto di rettificare o cancellare i dati personali o limitare il loro trattamento;
- diritto di proporre reclamo all'autorità di controllo;
- tutte le informazioni disponibili sulle fonti dei dati oggetto del trattamento, qualora i dati non siano raccolti presso l'interessato;
- nel caso di decisioni automatizzate, la logica applicata nei trattamenti automatizzati dei dati.

3.2. DIRITTO DI RETTIFICA (ART. 16 GDPR)

L'interessato può chiedere al titolare di correggere le inesattezze dei dati personali che lo riguardano. Le inesattezze possono riguardare anche l'incompletezza dei dati stessi; in questo caso l'interessato potrà chiedere al titolare l'integrazione dei dati, anche mediante una dichiarazione specifica.

I dati personali dovranno essere rettificati senza ingiustificato ritardo, a meno che la richiesta di rettifica non sia correlata a questioni giuridicamente rilevanti, legittimando il titolare a richiedere la prova delle presunte inesattezze.

3.3. DIRITTO ALLA CANCELLAZIONE (ART. 17 GDPR)

Garantire agli interessati il diritto alla cancellazione, c.d. diritto all'oblio, significa rendere efficaci i principi di protezione dei dati, soprattutto nell'ambiente online.

Il titolare è tenuto a dare corso alla richiesta di cancellazione dei dati, senza ingiustificato ritardo quando:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- i dati personali sono raccolti relativamente all'offerta di servizi della società dell'informazione a minori, ai sensi dell'art. 8 GDPR.

La prova della legittimità del trattamento è in capo al titolare del trattamento, il quale, inoltre, deve sempre essere in grado di provare l'esistenza di una solida base giuridica per il trattamento dei dati, in virtù del principio di responsabilizzazione.

Il diritto alla cancellazione non è privo di eccezioni, connesse ai casi in cui il trattamento dei dati personali sia necessario per:

- l'esercizio del diritto alla libertà di espressione e di informazione;
- l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

- motivi di interesse pubblico nel settore della sanità pubblica;
- fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il Gruppo WP29 ha adottato delle linee guida⁸ nelle quali ricorda, fra gli altri, che il diritto all'oblio non è assoluto, va ponderato con gli altri diritti e, quindi, il risultato di una richiesta può variare a seconda del caso in questione.

Se il titolare ha reso pubblici i dati oggetto della richiesta di cancellazione, ha l'obbligo di ottemperare alla richiesta e adottare misure ragionevoli per informare gli altri titolari del trattamento dei medesimi dati circa la richiesta di cancellazione, tenendo conto anche delle tecnologie disponibili e dei costi di attuazione.

3.4. DIRITTO DI LIMITAZIONE DI TRATTAMENTO (ART. 18 GDPR)

Gli interessati possono chiedere la limitazione del trattamento quando:

- viene contestata l'esattezza dei dati personali;
- il trattamento è illecito e l'interessato chiede la limitazione dell'utilizzo dei dati personali invece della cancellazione;
- i dati devono essere conservati per l'esercizio o la difesa di un diritto in sede giudiziaria;
- è pendente una decisione in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

In caso di revoca della limitazione, il titolare è tenuto a informare l'interessato prima di effettuare tale revoca. Eventuali rettifiche o cancellazioni dei dati personali o limitazioni del trattamento devono essere comunicate dal titolare a ciascuno dei destinatari a cui sono stati trasmessi i dati, a meno che ciò non risulti impossibile o sproporzionato (art. 19 GDPR). L'interessato può chiedere al titolare di fornire le informazioni riguardanti tali destinatari e il titolare è tenuto a fornirglielie.

A titolo di esempio, un titolare del trattamento può limitare il trattamento dei dati personali trasferendo temporaneamente i dati selezionati verso un altro sistema di trattamento, renderli inaccessibili agli utenti o rimuoverli temporaneamente.

8. Gruppo di lavoro articolo 29, *Linee guida relative all'esecuzione della sentenza della CGUE nella causa "Google Spain et Inc. c. Agencia Espanola de Proteccion de Datos (AEPD) e Mario Costeja Gonzalez" C-131/12, WP 225, Bruxelles, 26 novembre 2014*

3.5. DIRITTO ALLA PORTABILITÀ DEI DATI (ART. 20 GDPR)

Gli interessati possono esercitare il diritto alla portabilità dei dati trattati con mezzi automatizzati e sulla base del consenso o per l'esecuzione di un contratto. Questo significa che il diritto alla portabilità dei dati non si applica qualora il trattamento dei dati personali si basi su un fondamento giuridico diverso dal consenso o contratto.

Gli interessati hanno il diritto di ottenere la trasmissione diretta dei loro dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. A tal fine, il titolare del trattamento deve sviluppare formati interoperabili che consentano la portabilità dei dati. Per interoperabilità s'intende la capacità di sistemi di informazione e comunicazione, di interagire e scambiare dati e informazioni senza vincoli sulle implementazioni mediante protocolli sviluppati a tale scopo. Il GDPR non impone l'utilizzo di un formato specifico.

3.6. DIRITTO DI OPPOSIZIONE (ART. 21 GDPR)

Il diritto di opposizione è riconosciuto agli interessati che si trovano in particolari condizioni, quando la base giuridica del trattamento è l'esecuzione da parte del titolare di un compito svolto nel pubblico interesse o il legittimo interesse del titolare stesso, compresa la profilazione fondata su tali basi giuridiche.

Nell'esercizio del diritto di opposizione per particolari motivi occorre valutare il bilanciamento tra i diritti di protezione dei dati dell'interessato e i motivi legittimi (che devono essere "cogenti", come specificato dall'art. 21 del GDPR) per i quali il titolare intenderebbe continuare a trattare tali dati. L'onere della prova spetta, dunque, al titolare, il quale dovrà dimostrare l'esistenza di motivi cogenti per continuare il trattamento.

Una volta accolta un'opposizione, il titolare non può più trattare i dati dell'opponente. Resteranno valide, tuttavia, tutte le operazioni svolte prima dell'opposizione.

L'art. 21 del GDPR, al paragrafo 2, prevede il diritto di opporsi all'ulteriore trattamento dei dati per finalità di **marketing diretto** (su cui si tornerà più avanti), in qualsiasi momento e gratuitamente. Gli interessati devono essere informati di tale diritto chiaramente e separatamente da qualsiasi altra informazione.

L'opposizione ai dati personali trattati nell'ambito di **servizi della società dell'informazione**, ossia quelli prestati normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi, può avvenire con mezzi automatici.

I titolari che offrono tali servizi devono mettere in atto misure e procedure tecniche adeguate per garantire che il diritto di opposizione con mezzi automatizzati possa essere esercitato in modo efficace (ad es. bloccando i cookies nelle pagine web). Infine, qualora i dati personali siano trattati a fini di ricerca scientifica, storica o per finalità statistiche, l'interessato può opporsi per motivi connessi alla sua situazione particolare, a meno che il trattamento non sia necessario per l'esecuzione di un compito di interesse pubblico.

3.7. PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE, COMPRESA LA PROFILAZIONE (ART. 22 GDPR)

Le decisioni automatizzate, adottate sulla base di dati personali trattati esclusivamente con mezzi automatici, possono produrre effetti giuridici o incidere significativamente sulle vite delle persone fisiche. L'art. 22, par. 1, GDPR, vieta un siffatto utilizzo delle decisioni automatizzate, a meno che esse:

- siano necessarie per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento;
- siano autorizzate dal diritto dell'Unione o dello Stato membro, purché i diritti, le libertà e i legittimi interessi dell'interessato siano adeguatamente garantiti;
- si basino sul consenso esplicito dell'interessato.

Tra i trattamenti automatizzati rientra la **profilazione**, cioè quella forma di valutazione automatizzata degli “aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”⁹.

Se ammesse, le decisioni automatizzate devono essere accompagnate da misure appropriate adottate dal titolare del trattamento per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, comprendenti almeno il diritto di ottenere l'intervento umano da parte del titolare, di esprimere la propria opinione e di contestare la decisione.



È possibile scaricare dal sito del Garante il modello per l'esercizio dei diritti in materia di protezione dei dati personali (<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924>)

⁹. Si veda in proposito l'art. 4, par. 4, GDPR e il considerando n. 71.



*Marketing
e profilazione*

1. COME DISTINGUERE IL MARKETING DALLA PROFILAZIONE

Si annovera tra le attività di marketing tutto ciò che riguarda l'analisi di dati per collocare prodotti o servizi in un dato mercato, attraverso differenti strumenti: comunicazione commerciale, invio di materiale pubblicitario, vendita diretta. Il consenso richiesto per le attività di marketing riguarda l'uso dei dati anagrafici e di contatto (nome, cognome, numero di telefono, e-mail), ma non sempre deve essere richiesto (si veda paragrafo successivo).

La profilazione, invece, ha quale scopo quello di anticipare le scelte delle persone attraverso un'analisi delle abitudini di consumo e il monitoraggio sull'uso dei siti e dei servizi di comunicazione web.

In tal caso il consenso attiene all'uso di informazioni aggiuntive rispetto a quelle anagrafiche e di contatto, come ad esempio il titolo di studio, il nucleo familiare, le risposte a questionari sui consumi o i dati di comportamenti reali di acquisto.

Tipico strumento di profilazione sono i cookies detti appunto di profilazione, con i quali i siti visitati tracciano la navigazione dell'utente in rete e creano profili sui suoi gusti, abitudini, scelte, in modo da poter inviare all'utente messaggi pubblicitari in linea con le preferenze già manifestate dallo stesso utente.

2. IL CONSENSO NELLE ATTIVITÀ DI MARKETING DIRETTO (“SOFT SPAM”)

Il *direct marketing*, con le quali le imprese, ma anche gli enti, comunicano direttamente con un cliente o un gruppo determinato di clienti, è generalmente subordinato al consenso dell'interessato quando è effettuato con sistemi automatizzati di chiamata o nell'ambito di comunicazioni elettroniche, attraverso posta elettronica, telefax, Mms, Sms o altro tipo di strumenti (art. 130, commi 1 e 2, D.Lgs. 196/2003).

Il consenso non è richiesto tutte le volte che il titolare del trattamento utilizza l'indirizzo di posta elettronica, **in precedenza fornito dall'interessato nel contesto della vendita di un prodotto o di un servizio**, per finalità di vendita diretta di propri prodotti o servizi (art. 130, c. 4, D.Lgs. 196/2003).

Il titolare ha in tal caso un legittimo interesse (art. 6, par. 1, lett. f e C. 47, ultimo periodo, GDPR) al trattamento dei dati personali dell'interessato, a condizione che:

- si tratti di **servizi analoghi** a quelli oggetto della vendita;

- l'interessato, al quale il titolare abbia fornito tutte le informazioni, non rifiuti l'uso dei dati per finalità di marketing diretto, fin dall'inizio o successivamente (c.d. **opt-out**).

Le informazioni sulla possibilità di opporsi al trattamento per la vendita diretta devono essere rese sia al momento della raccolta che in occasione dell'invio di ogni comunicazione. L'opposizione deve poter avvenire in maniera agevole e gratuitamente, ad esempio attraverso un'apposita opzione "cancellami".

Non sarebbe conforme alla legge, quindi, un sistema che richiede il compimento di numerose operazioni, con continui rinvii a link diversi, per poter esercitare il diritto di opposizione al trattamento.

3. NEWSLETTER. ADEMPIMENTI PER UNA CORRETTA GESTIONE

L'iscrizione ad una lista di contatti (newsletter) è un'opzione largamente utilizzata dalle imprese per mantenere un contatto con i propri clienti, inviando informazioni e aggiornamenti sulle attività, i prodotti o i servizi offerti. Data l'importanza di questo strumento per fidelizzare il cliente, spesso le imprese tendono a iscrivere i clienti a tali liste in maniera automatica, prevedendo dei form in cui il consenso è espresso di default, con la relativa casella già pre-selezionata.

Inutile dire che la pratica appena descritta non è conforme alla normativa. La legge, infatti, prevede un sistema di **opt-in**, mediante il quale l'interessato esprima un consenso esplicito e libero all'iscrizione a una newsletter, inserendo il proprio indirizzo mail e cliccando sul tasto "iscrivimi" (o analogo).

Per evitare che un terzo si iscriva a un servizio all'insaputa dell'interessato di cui si utilizzano i dati (es. nome, cognome, e-mail e altri dati di contatto), sarebbe preferibile adottare un sistema c.d. di **double opt-in**: l'utente inserisce il proprio indirizzo e-mail nell'apposito box e clicca "iscrivimi" (prima manifestazione di consenso) ottenendo in cambio un messaggio del servizio di gestione (inviato all'indirizzo e-mail utilizzato) contenente un link speciale. Il click dell'utente su questo link corrisponde alla seconda manifestazione esplicita di consenso ed è quello che effettivamente iscrive l'indirizzo e-mail alla lista.

4. INFORMATIVA MULTISTRATO PER I PROCESSI DECISIONALI AUTOMATIZZATI (COMPRESA LA PROFILAZIONE)

Quando si utilizza un processo decisionale automatizzato (compresa la profilazione), il titolare dovrà darne atto nell’informativa, indicando il tipo di processo decisionale automatizzato utilizzato, quale sia la logica sottesa a tale processo e le conseguenze del trattamento.

Per rendere l’informativa accessibile ed efficace può essere utile adottare un approccio “multistrato”¹⁰, in cui le informazioni sono rese su due distinti livelli.

Il **primo livello** contiene le informazioni più rilevanti per gli utenti:

- Trattamenti dei dati personali effettuati;
- Tipologie dei dati trattati;
- Finalità del trattamento;
- Indicazione del titolare;
- Ambito di circolazione dei dati;
- Modalità di esercizio dei diritti degli interessati.

Il **secondo livello** contiene la policy relativa a specifiche funzionalità e la formulazione di esempi per chiarire le modalità del trattamento dei dati.

5. ACQUISIZIONE DEL CONSENSO IN CASO DI PROFILAZIONE DI UTENTI NON AUTENTICATI

Esiste un’importante distinzione fra gli utenti che fruiscono dei servizi offerti online e che incide sulle modalità di acquisizione del consenso. Coloro che dispongono di un account creato a seguito di una procedura di registrazione per l’accesso “autenticato” ai servizi sono i cc.dd. utenti autenticati, ad esempio per il servizio di posta elettronica, mentre quelli che non hanno un account sono detti utenti non autenticati.

Questi ultimi non hanno avuto modo di esprimere il consenso al trattamento dei dati per finalità di profilazione, pertanto si deve prevedere, nella fruizione di funzionalità del servizio, uno spazio idoneo a consentire loro di esprimere il consenso, altrimenti gli stessi utenti non autenticati - accedendo alla prima pagina del sito - devono visualizzare in primo piano un’area contenente, in alternativa:

- l’indicazione che il titolare effettua il trattamento per finalità di profilazione;

¹⁰. Si v. “Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015” (Pubblicato sulla Gazzetta Ufficiale n. 103 del 6 maggio 2015).

- il link all’informativa;
- il link ad apposita area dove sia possibile negare, integralmente o in maniera modulare, il consenso alla profilazione
- indicazione che proseguendo con la navigazione si presta il consenso.

L’Autorità Garante per la protezione dei dati personali¹¹ ha inoltre precisato che:

- occorre un meccanismo idoneo a consentire l’espressione del consenso di cui sarà tenuta traccia (ad es. mediante cookie tecnici) tramite una azione proattiva dell’interessato;
- se l’utente presta il consenso, il meccanismo non dovrà essere riproposto nelle sue visite successive;
- se l’utente ha solo seguito il link all’informativa il meccanismo dovrà essere riproposto successivamente;
- se l’utente ha solo seguito il link alla modulazione delle scelte sulla profilazione, queste dovranno essere memorizzate in dettaglio.

¹¹. *Ibid.*



*Analisi del sito web
aziendale*

1. COSA SONO E A COSA SERVONO I COOKIE

I cookie sono delle informazioni contenute in piccoli file di testo che i siti visitati dagli utenti inviano ai loro dispositivi (personal computer, tablet, smartphone o altri device), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti nelle visite successive. Di solito, queste piccole stringhe di testo vengono memorizzate nel browser degli utenti con lo scopo di essere poi ritrasmesse al sito nel corso delle successive visite.

L'utente può ricevere sul suo terminale anche cookie di siti o di web server diversi (c.d. cookie di "terze parti") e questo accade perché sul sito web visitato sono presenti elementi come, ad esempio, immagini, mappe, suoni, specifici link a pagine web di altri domini che risiedono su server diversi da quello sul quale si trova la pagina richiesta.

I cookie possono avere finalità molto differenti dalle quali derivano diversi effetti e criticità nell'utilizzo degli stessi. Sono usati per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazioni di informazioni specifiche riguardanti gli utenti che accedono ai server.

2. TIPOLOGIE DI COOKIE

Come già riferito, esistono diversi tipi di cookie che svolgono differenti funzioni e ai quali si applicano regole diverse, a seconda che interferiscano o meno con i diritti e le libertà degli utenti.

2.1 COOKIE TECNICI

Sono utilizzati al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione, esplicitamente richiesto dall'abbonato o dall'utente, a erogare tale servizio.

I cookie tecnici possono essere ulteriormente distinti in:

• **Cookie di navigazione**

Sono quelli che consentono al sito di funzionare correttamente, permettendo la navigazione e la fornitura di servizi richiesti dall'utente. Essi sono temporanei e vengono cancellati al termine del periodo di durata.

Senza il ricorso a tale tipo di cookie alcune operazioni sarebbero meno sicure o più complesse e, in alcuni casi, non potrebbero proprio essere compiute.

• **Cookie funzionali**

Sono quelli che consentono al sito, in base alle indicazioni dell'utente, di memorizzare alcune delle informazioni della navigazione effettuata dallo stesso, al fine di essere riutilizzate nelle navigazioni successive, migliorando il servizio offerto e la qualità della navigazione.

• **Cookie analitici**

Sono utilizzati per raccogliere informazioni, in forma aggregata, al fine di condurre analisi statistiche delle modalità di navigazione del sito. Sono dati anonimi, di solito utilizzati per migliorare le funzionalità del sito tramite la raccolta dei dati dell'utenza che lo utilizza, e possono essere assimilati ai cookie tecnici solo se utilizzati al fine di un'ottimizzazione del sito da parte del gestore dello stesso.

2.2 COOKIE DI PROFILAZIONE

Utilizzati per tracciare le abitudini di navigazione degli utenti con lo scopo di creare profili dei loro gusti, delle loro abitudini, delle scelte prese o di altre informazioni. La finalità è di inviare all'utente profilato messaggi pubblicitari mirati, in linea con le preferenze manifestate dallo stesso durante la navigazione.

I cookie possono essere installati dal gestore del sito che l'utente sta visitando (che può essere indicato anche come "editore"). Si parla in tali casi di **cookie di prima parte**. Quando è un soggetto proprietario di un sito diverso che installa cookie per il tramite del sito editore si è di fronte, invece, a **cookie di terze parti**.

3. COOKIE E CONSENSO

La classificazione dei cookie appena fatta permette di comprendere quando è necessario richiedere il consenso dell'utente. La Commissione europea e l'Autorità Garante per la protezione dei dati personali hanno, infatti, individuato quattro categorie di cookie in base alle quali modulare la prestazione del consenso.

<i>Strictly necessary cookies</i>	Senza questi cookie la trasmissione di una comunicazione su rete elettronica non sarebbe possibile. Questi sono collegati a un servizio espressamente richiesto dal visitatore, es. quelli del carrello virtuale nei siti di e-commerce	NON è necessario il consenso
<i>Performance cookies</i>	Questi cookie raccolgono informazioni sull'uso del sito da parte dei visitatori, in maniera anonima e senza profilazione (es. Google Analytics, advertising e pay per click).	Se trattano dati in forma anonima e aggregata NON è necessario il consenso.
<i>Functionality cookies</i>	Servono a ricordare le scelte dell'utente e automatizzano alcune procedure (come il login) oppure personalizzano l'accesso e la navigazione del sito (es. lingua dell'utente)	NON è necessario il consenso
<i>Targeting o advertising cookies</i>	Cookie pubblicitari che consentono la profilazione degli utenti al fine di fornire pubblicità mirata, legati spesso a siti di terze parti, che raccolgono informazioni relative alla navigazione degli utenti.	Necessario il consenso

4. INFORMATIVE E MANIFESTAZIONE DEL CONSENSO

Il primo accesso alla home page o a qualunque altra pagina di un sito web deve essere sempre preceduto da un **banner**, se si utilizzano cookie di profilazione (di prima e/o di terza parte).

Nel caso in cui si utilizzino solo cookie tecnici è sufficiente la sola **informativa estesa**, che fornisca informazioni circa l'utilizzo e le finalità dei cookie presenti sul sito.

Il banner deve comparire in primo piano e presentare dei colori e dei caratteri

tali da rendere percettibile la discontinuità nella fruizione dei contenuti della pagina web che si sta visitando, senza impedire le interazioni con la pagina stessa.

Esso conterrà le seguenti indicazioni:

- che il sito utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete;
- che il sito consente anche l'invio di cookie di "terze parti" (laddove si verifichi);
- il link all'informativa estesa, ove vengono fornite indicazioni sull'uso dei cookie tecnici e analytics, dando la possibilità di scegliere quali specifici cookie autorizzare;
- l'indicazione che alla pagina dell'informativa estesa (linkabile da ogni pagina del sito e posta in calce ad essa) è possibile negare il consenso all'installazione di qualunque cookie;
- l'indicazione che costituisce accettazione dei cookie la prosecuzione della navigazione mediante accesso ad altra area del sito, la selezione di un elemento dello stesso (ad esempio di un'immagine o di un link), l'eventuale chiusura del banner facendo click sulla "X" o lo scorrimento della pagina (scroll).

La prestazione del consenso è registrata e conservata dall'editore mediante l'utilizzo di un cookie tecnico. Ciò permetterà di non riproporre l'informativa breve alla seconda visita del sito, benché l'utente possa in qualunque momento modificare o negare il consenso rispetto all'utilizzo dei cookie.

Non esiste una soluzione tecnologica di semplice applicazione che dia la certezza dell'avvenuta prestazione del consenso da parte dell'utente. Per questo si suggerisce al titolare /gestore del sito di:

- prevedere un sistema di risposta all'utente, il quale in caso di lamentela dovrà al più presto ricevere un riscontro su come esercitare il proprio consenso/diniego selettivo o come cancellare i cookie dal proprio browser, prevedendo all'occorrenza apposite pagine informative;
- predisporre una sorta di certificazione del processo di acquisizione e conservazione del cookie tecnico del consenso (ad es. registrando le azioni con le quali l'utente manifesta il proprio consenso all'utilizzo dei cookie e, unitamente a queste, memorizzando, o comunque rendendo disponibile in fase di controllo, anche l'informativa a seguito della quale l'utente ha prestato il proprio consenso).

5. CONTENUTO DELLA COOKIE POLICY

L'informativa estesa o cookie policy (accessibile da ogni pagina del sito, sia dagli utenti registrati che da quelli non registrati) contiene tutti gli elementi di cui all'art. 13 GDPR. Inoltre, devono essere presenti:

- una spiegazione generale di cosa sono i cookie e della gestione degli stessi tramite le impostazioni dei browser;
- la descrizione delle categorie di cookie tecnici suddivisi per finalità;
- la spiegazione di come viene prestato il consenso (scroll, tasto “ok” o “X”, link);
- la descrizione dei cookie di profilazione di prima parte, con il relativo modulo di consenso;
- le informazioni relative alla profilazione sia degli utenti registrati che non¹²;
- la descrizione delle finalità dei cookie di terza parte.

All'interno di tale informativa deve essere inserito anche il link aggiornato alle informative e ai moduli di consenso delle terze parti con le quali l'editore ha stipulato accordi per l'installazione di cookie tramite il proprio sito (qualora l'editore abbia contatti indiretti con le terze parti, dovrà linkare i siti dei soggetti che fanno da intermediari tra lui e le stesse terze parti).

Al fine di mantenere distinta la responsabilità degli editori da quella delle terze parti in relazione all'informativa resa e al consenso acquisito per i cookie di queste ultime tramite il proprio sito, gli editori devono acquisire, già in fase contrattuale, il link dalle terze parti (con ciò intendendosi anche gli stessi concessionari).

Si ricorda, infine, che nel medesimo spazio dell'informativa estesa deve essere richiamata la possibilità per l'utente (art. 122, c. 2, D.Lgs. 196/2003) di manifestare le proprie opzioni in merito all'uso dei cookie da parte del sito anche attraverso le impostazioni del browser, indicando almeno la procedura da seguire per configurare tali impostazioni. Qualora, poi, le tecnologie utilizzate dal sito siano compatibili con la versione del browser utilizzata dall'utente, l'editore potrà predisporre un collegamento diretto con la sezione del browser dedicata alle impostazioni stesse.

È bene notare che se l'utente non interagisce con i moduli del consenso ed esce dall'informativa stessa, chiudendola o proseguendo la navigazione del sito, di fatto presta il consenso per tutti i cookie, a condizione, però, che nell'informativa estesa sia stata inserita questa indicazione in maniera esplicita e trasparente.

¹². V. anche *supra*, **Cap. II, par. 5**.

IV *Il Registro delle attività di trattamento*

1. NATURA E FUNZIONI DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

I contenuti del Registro sono fissati nell'articolo 30 GDPR. Tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

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

Il Registro assolve ad una doppia funzione:

a) È uno **strumento operativo** che consente di:

- **censire le banche dati e i trattamenti** in essere;
- **rappresentare l'organizzazione** sotto il profilo delle attività di trattamento a fini di **informazione, consapevolezza e condivisione interna**;
- costituire lo **strumento di pianificazione e controllo** delle attività di trattamento dei dati personali in modo da garantire la loro **integrità, riservatezza e disponibilità**;
- ridurre gli sprechi in termini di tempo, risorse, duplicazione delle informazioni;
- ridurre i rischi di eventuali trattamenti illeciti.

b) Consente l'**archiviazione** in maniera **ordinata, organizzata e verificabile** da terzi **delle informazioni relative all'adozione delle misure tecniche ed organizzative adeguate** ed efficaci finalizzate ad attuare il principio di accountability.

La tenuta dei registri in forma scritta (anche in formato elettronico), da parte del titolare e del responsabile del trattamento, permette di dimostrare la legittimità del trattamento e assolvere all'onere della prova, tutte le volte in cui debba essere valutata la responsabilità del titolare e/o del responsabile (art. 30, c.3, GDPR). Infatti, su richiesta dell'autorità di controllo, tale Registro deve essere messo a sua disposizione (art. 30, c.4, GDPR).

2. OBBLIGO DI TENUTA DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

I titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle

attività di trattamento In particolare, ricorre l'obbligo di tenuta del Registro per:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 GDPR, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR.

Rientrano nella categoria delle “organizzazioni” di cui all'art. 30, par. 5 anche le associazioni, fondazioni e i comitati.

Alla luce di quanto detto sopra, sono tenuti all'obbligo di redazione del Registro, ad esempio:

- **esercizi commerciali, esercizi pubblici o artigiani** con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);

- **liberi professionisti** con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);

- **associazioni, fondazioni e comitati** ove trattino “categorie particolari di dati” e/o dati relativi a condanne penali o reati (ad es. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. “vulnerabili” quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);

- i **condomini** ove trattino “categorie particolari di dati” (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Infine, si precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del Registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del Registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti a un

solo lavoratore dipendente, il Registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

Al di fuori dei casi di tenuta obbligatoria del Registro, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso¹³.

3. CONTENUTI DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Le informazioni che il Registro delle attività di trattamento del titolare deve contenere sono indicate all'art. 30, par. 1, lett. a – g, GDPR, ossia:

- a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del controllore del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

È opportuno considerare di inserire nel Registro anche le seguenti informazioni:

- attività effettuate
- base giuridica del trattamento
- elenco terzi coinvolti
- analisi del rischio per singolo applicativo e/o servizio
- esistenza di valutazione d'impatto e consultazione preventiva
- documentazione a supporto del trattamento (es. informativa e consenso)

¹³. Si veda Considerando 82, GDPR.

- procedure per l'esercizio dei diritti dell'interessato
- provvedimenti specifici dell'autorità di controllo.

Il GDPR non prevede né un termine entro il quale aggiornare il Registro né un obbligo espresso di aggiornamento dello stesso. Tuttavia, sulla base del principio di accountability, il titolare è tenuto a garantire la conformità dei trattamenti al GDPR nonché essere in grado di dimostrarlo. Pertanto, spetterà al titolare approntare tutte le misure per garantire un costante aggiornamento del Registro.

Come già riferito, nulla toglie che possano essere riportate nel Registro informazioni ulteriori che il titolare o il responsabile ritengano utili (ad es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento ecc.).

4. MODALITÀ DI CONSERVAZIONE E AGGIORNAMENTO DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il Registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile. In quanto tale, il Registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il Registro può essere compilato sia in formato cartaceo che elettronico ma è assolutamente opportuno che esso in ogni caso rechi, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento. In quest'ultimo caso il Registro dovrà recare una annotazione del tipo:

- “- scheda creata in data XY”;
- “- ultimo aggiornamento avvenuto in data XY”.

5. IL REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

Il responsabile del trattamento tiene un Registro di “tutte le categorie di attività relative al trattamento svolte per conto di un titolare” (art. 30, par. 2 GDPR)¹⁴.

In merito alle modalità di compilazione dello stesso si rappresenta quanto segue:

a) nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari (es. società di software house), le informazioni di cui all'art. 30, par. 2 del RGPD dovranno essere riportate nel Registro con riferimento a ciascuno dei suddetti titolari. In questi casi il responsabile dovrà suddividere il Registro in tante sezioni quanti sono i titolari per conto dei quali agisce; ove, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi, nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi, risulti eccessivamente difficoltosa, il Registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, par. 2 del RGPD;

b) con riferimento alla “descrizione delle categorie di trattamenti effettuati” (art. 30, par. 2, lett. b), GDPR) è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell'art. 28, GDPR, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo;

14. a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

c) in caso di sub-responsabile, parimenti, il Registro delle attività di trattamento svolte da quest'ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell'art. 28, paragrafi 2 e 4, GDPR.



Dal sito del Garante è possibile scaricare il modello di “registro semplificato” delle attività di trattamento del titolare per PMI (<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048342>).

V *Accountability*
Privacy by design
e by default

1. IL CONCETTO DI ACCOUNTABILITY

Il termine *accountability* è mutuato dal mondo anglosassone e indica, in generale, l'obbligo di introdurre meccanismi di responsabilizzazione e controllo al fine di garantire un efficiente utilizzo delle risorse e la produzione di risultati, sia all'interno dell'azienda sia nei confronti degli "interessati" esterni all'azienda (cc.dd. *stakeholder*).

Nell'ottica della tutela dei dati personali, il principio di *accountability* prescrive in capo al titolare e al responsabile l'adozione di misure giuridiche, organizzative, tecniche, anche attraverso l'elaborazione di specifici modelli organizzativi (come quelli già approntati sulla base del D.Lgs. 231/2001, in materia di responsabilità amministrativa degli enti)¹⁵.

Pur potendo individuare degli specifici adempimenti¹⁶, a garanzia della certezza del diritto, il principio di responsabilità deve lasciare spazio a una certa adattabilità, che consenta di determinare le misure concrete da applicare in funzione dei rischi connessi al trattamento e dei tipi di dati trattati¹⁷.

Il principio di *accountability* mira a minimizzare i rischi per i diritti e le libertà fondamentali¹⁸. Non essendoci una definizione di rischio all'interno del GDPR, l'obbligo che incombe innanzitutto sul titolare del trattamento è permanente, necessita di revisioni periodiche che tengano conto di nuovi rischi o della presenza di misure più efficaci¹⁹.

2. SOGGETTI TENUTI AL RISPETTO DEL PRINCIPIO DI ACCOUNTABILITY

Il GDPR ha rovesciato la prospettiva della disciplina in materia di protezione dei dati personali in quanto tutto il nuovo quadro normativo è prevalentemente incentrato sui doveri e sulla responsabilizzazione del titolare del trattamento (e del responsabile).

Il titolare ha certo maggiore discrezionalità nel decidere in che modo conformarsi alle disposizioni del Regolamento, ma deve essere in grado di dimostrarlo (*compliance*).

¹⁵ V. Considerando n. 72 e art. 5, par. 2, GDPR.

¹⁶ Su cui v. oltre par. 3.

¹⁷ V. art. 24, par. 1, GDPR.

¹⁸ Fra questi la perdita del controllo dei dati personali, la limitazione dei diritti, la discriminazione, il furto o l'usurpazione di identità, le perdite finanziarie, ecc. (cfr. Considerando 75 e 85 GDPR).

¹⁹ Si vedano gli artt. 24, par. 1, 32, par. 1, lett. b) e 35, par. 11, GDPR.

Nessuno è escluso dall'obbligo di responsabilità, accanto al titolare anche il responsabile, il DPO e il personale incaricato devono farsi carico di conformare la loro attività alle prescrizioni del GDPR.

3. I PRINCIPALI ADEMPIMENTI RICHIESTI DAL PRINCIPIO DI ACCOUNTABILITY

L'accountability va ricercata in tutta la struttura del GDPR. A tal fine si dovrà procedere in una duplice direzione: tutelare l'interessato con procedure trasparenti, mediante informative ai dipendenti e ai clienti, convenzioni di contitolarità con i partner e accordi con i responsabili del trattamento (fornitori e/o consulenti), nonché definire i ruoli dei soggetti del trattamento dei dati, predisponendo i mansionari per dipendenti autorizzati al trattamento dei dati, indicando i designati e nominando, laddove sia necessario o comunque opportuno, il DPO.

In sintesi, le principali obbligazioni di compliance previste nel GDPR sono:

- Tenuta dei registri delle attività di trattamento, mediante i quali effettuare, tra l'altro, la mappatura dei trattamenti (art. 30)²⁰;
- Analisi dei rischi;
- La c.d. privacy by design e by default²¹;
- La predisposizione di idonee misure di sicurezza (art. 32);
- la valutazione d'impatto sulla protezione dei dati – DPIA – (art. 35);
- la consultazione preventiva dell'autorità di controllo (art. 36), qualora la valutazione d'impatto di cui all'art. 35 GDPR, mostri che il trattamento effettuato dal titolare presenterebbe un rischio elevato in assenza di misure adottate dallo stesso titolare per attenuarlo;
- la nomina di un DPO (artt. 37, 38 e 39);
- la notifica e la comunicazione di un "data breach" (artt. 33 e 34)²²;

4. PRIVACY BY DESIGN E BY DEFAULT

Le azioni volte alla protezione dei dati e alla tutela dei diritti e le libertà fondamentali sarebbero vanificate se non si intervenisse nel punto più prossimo al verificarsi di un rischio.

Già nel momento in cui si progetta un trattamento e nel corso dello stesso,

²⁰. Su cui v. *supra* Cap. IV.

²¹. V. par. 4.

²². V. Cap. VIII

il titolare predispone misure tecniche e organizzative adeguate (es. la pseudonimizzazione), affinché siano attuati i principi di protezione dei dati (ad es. la minimizzazione), oltre alle garanzie di tutela dei diritti degli interessati. La scelta delle misure di sicurezza tecniche e organizzative adeguate che il titolare e il responsabile vorranno adottare deve essere effettuata in relazione a diversi fattori, fra i quali:

- lo stato dell'arte e dei costi di attuazione di una misura;
- la natura, l'ambito di applicazione, il contesto e le finalità della soluzione in fase di progettazione che include il trattamento di dati personali;
- tutti i rischi di violazione delle disposizioni del GDPR o delle garanzie per i diritti delle persone interessate, incluse le diverse probabilità e gravità dei rischi.

Impedire per impostazione predefinita che i dati personali non necessari alla specifica finalità del trattamento siano trattati per l'erogazione di un determinato servizio, ad esempio, costituisce un esempio di come approntare misure tecniche e organizzative adeguate (c.d. *privacy by default*). In particolare, tale obbligo riguarda la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

L'approccio da seguire è quello della neutralità tecnologica e dunque metodologico, sulla scorta dei seguenti principi:

- **proattività e non reattività** – prevenire non correggere, cioè i problemi vanno valutati nella fase di progettazione, e l'applicativo deve prevenire il verificarsi dei rischi;
- **privacy come impostazione di default** (ad esempio, non deve essere obbligatorio compilare il campo di un *form* il cui conferimento di dati è facoltativo);
- **privacy incorporata nella progettazione** (ad esempio, l'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati);
- **massima funzionalità**, in modo da rispettare tutte le esigenze;
- **sicurezza fino alla fine** – piena protezione del ciclo vitale (del trattamento);
- **visibilità e trasparenza**, cioè tutte le fasi operative devono essere trasparenti in modo che sia verificabile la tutela dei dati personali;
- **centralità dell'utente**, quindi rispetto dei suoi diritti, tempestive e chiare risposte alle sue richieste di accesso.

VI *Le Informative Privacy*

1. PERCHÉ È IMPORTANTE FORNIRE LE INFORMATIVE PRIVACY

Il titolare del trattamento adotta le misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare per quelle informazioni destinate ai minori.

Le informazioni sono in genere fornite per iscritto o con altri mezzi, ivi compresi mezzi elettronici. Nulla esclude che queste informazioni possano essere fornite oralmente, su richiesta dell'interessato e sempreché sia comprovata con altri mezzi l'identità dell'interessato stesso²³.

Il legislatore europeo ha preso molto sul serio il rispetto degli obblighi di trasparenza, prevedendo, da un lato, la responsabilizzazione del titolare (e del responsabile), a cui è demandata la predisposizione di misure adeguate ad assicurare fra gli altri il principio di trasparenza, dall'altro, sanzionando l'inosservanza degli obblighi informativi con **sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente se superiore**.

Pertanto, le informative sono il punto di arrivo di un percorso basato sull'analisi e la mappatura dei trattamenti dei dati personali riguardanti la propria organizzazione, anche se affidati all'esterno.

2. DATI RACCOLTI PRESSO L'INTERESSATO (art. 13, par. 1 e 2): QUALI INFORMAZIONI FORNIRE

Nel momento in cui i dati personali sono ottenuti, il titolare del trattamento ha l'obbligo di fornire le informazioni di cui all'art. 13, par. 1 e 2:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante. Il rappresentante è la persona fisica o giuridica che è designata dal titolare del trattamento o dal responsabile del trattamento che non sono stabiliti nell'Unione e li rappresenta per quanto riguarda gli obblighi rispettivi a norma del Regolamento²⁴;
- i dati di contatto dell'eventuale responsabile della protezione dei dati (*Data Protection Officer* – DPO), in quanto punto di contatto anche rispetto agli interessati;

23. V. art. 12, par. 1, GDPR.

24. V. art. 4, n. 17, GDPR.

- la finalità e la base giuridica del trattamento. Se il trattamento è necessario per il perseguimento del legittimo interesse²⁵ del titolare o di terzi, questi deve essere specificato;
- gli eventuali **destinatari** o le eventuali **categorie di destinatari** dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento **di trasferire dati personali a un paese terzo** (*non appartenente all'UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein*) o a un'**organizzazione internazionale** e l'indicazione delle condizioni che legittimano il trasferimento, previste dal Regolamento al fine di assicurare che il livello di protezione delle persone fisiche garantito dallo stesso non sia pregiudicato²⁶ ;
- il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo²⁷ ;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'**accesso** ai dati personali e la **rettifica** o la **cancellazione** degli stessi o la **limitazione** del trattamento dei dati

25. Cfr. nota n. 2

26. Tali condizioni, che devono essere indicate nell'informativa, stabilite in ordine gerarchico, sono:

a) l'esistenza di una decisione di adeguatezza della Commissione;

b) in assenza di decisioni di adeguatezza della Commissione, il riferimento a garanzie adeguate che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa, le clausole contrattuali tipo approvate dalla Commissione l'osservanza di un codice di condotta o di un meccanismo di certificazione) e l'indicazione dei mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili;

c) in assenza di ogni altro presupposto, il riferimento alle condizioni, applicabili in specifiche situazioni, che legittimano il trasferimento a norma dell'art. 49 del Regolamento (ad esempio, la prestazione del consenso esplicito dell'interessato, che abbia ricevuto tutte le informazioni necessarie sui rischi associati al trasferimento).

27.

ESEMPIO

Periodo di conservazione dei dati.

I dati oggetto di trattamento saranno conservati per un periodo di tempo non superiore a quello necessario a conseguire gli scopi per i quali essi sono stati raccolti o successivamente trattati e, in particolare:

- *i dati forniti mediante l'invio di messaggi di posta elettronica o la compilazione dei form di contatto presenti sul sito saranno conservati per il tempo necessario a fornire riscontro;*
- *i dati forniti ai fini dell'iscrizione al servizio di newsletter saranno trattati fino ad eventuale esercizio del diritto di opposizione ex 21 del GDPR da parte dell'interessato;*
- *i dati forniti mediante compilazione del form presente nella sezione "lavora con noi" saranno conservati per un periodo massimo di 12 mesi dal loro conferimento e potranno essere utilizzati per eventuali contatti finalizzate a successive selezioni;*
- *i dati forniti per la presentazione della richiesta di iscrizione al Mastercourse ANORC, saranno conservati fino al perfezionamento della procedura di iscrizione.*

Il Titolare provvederà, dopo la decorrenza dei termini di conservazione secondo gli indicati criteri, ad adottare misure preordinate alla cancellazione o all'anonimizzazione dei dati che non debbano essere conservati per specifici obblighi di normativi.

- qualora il trattamento sia basato sul consenso espresso dall'interessato, l'esistenza del diritto **di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre **reclamo** a un'autorità di controllo (in Italia il Garante per la protezione dei dati personali);
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le **possibili conseguenze della mancata comunicazione di tali dati**;
- l'esistenza di un **processo decisionale automatizzato**, compresa la **profilazione** e, almeno in questo caso, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato²⁸.

Tale obbligo conosce un'**eccezione**: il titolare del trattamento può evitare di fornire l'informativa qualora l'interessato disponga già delle informazioni.

In caso di **contitolarità**, i contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive funzioni di comunicazione delle informazioni agli interessati. Tale accordo può designare un punto di contatto per gli interessati.

3. DATI RACCOLTI PRESSO L'INTERESSATO: TRATTAMENTO PER FINALITÀ DIVERSA

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una **finalità diversa** da quella per cui sono stati raccolti, deve fornire all'interessato le seguenti **ulteriori informazioni**:

- indicazione della **nuova finalità**;
- **periodo di conservazione** dei dati personali o, quando non è possibile i criteri utilizzati per determinare tale periodo;
- **eventuale processo decisionale** basato unicamente su trattamento automatizzato, **logica** utilizzata e **conseguenze** per l'interessato;
- **diritti dell'interessato**: accesso, rettifica/integrazione, cancellazione, limitazione, opposizione, portabilità, reclamo a un'Autorità garante, revoca del consenso nei casi di legge.

28. Sulla profilazione v. supra Cap I, par. 3, n. 7 e Cap. II

4. DATI RACCOLTI PRESSO SOGGETTO DIVERSO DALL'INTERESSATO (art. 14)

In questo caso il contenuto dell'informativa è lo stesso di quella fornita ai sensi dell'art. 13, alla quale vanno aggiunte le seguenti indicazioni:

- **origine** dei dati personali, precisando se gli stessi provengano eventualmente da fonti accessibili al pubblico;
- **categorie** di dati personali trattati.

Il titolare fornisce le informazioni previste all'art. 14, par. 1 e 2:

- **entro un termine ragionevole** dall'ottenimento dei dati personali, ma al più tardi **entro un mese**, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- nel caso in cui i dati personali siano **destinati alla comunicazione con l'interessato**, al più tardi **al momento della prima comunicazione dall'interessato**;
- nel caso sia prevista la **comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali**.

È possibile non fornire l'informativa quando:

- risulta impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In questi casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
- i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

VIII

*DPO: Ruolo, Compiti
e Funzioni*

1. QUALI SONO I COMPITI CHE IL DPO È CHIAMATO A SVOLGERE

Il DPO svolge compiti di consulenza, audit e controllo all'interno dell'impresa o ente. In particolare, il DPO:

- informa e fornisce consulenza al titolare e al responsabile, ma anche ai dipendenti che eseguono il trattamento, in merito agli obblighi previsti in materia di protezione dei dati personali;
- sorveglia l'osservanza dei predetti obblighi e degli eventuali disciplinari interni, incluso l'attribuzione delle responsabilità e anche la sensibilizzazione e formazione del personale;
- fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati personali e ne sorveglia lo svolgimento ai sensi dell'art. 35;
- coopera con l'autorità di controllo e funge da punto di contatto con la stessa per tutte le questioni connesse al trattamento dei dati personali, inclusa la consultazione preventiva di cui all'art. 36 GDPR.

Nulla vieta al titolare o al responsabile del trattamento di affidare al DPO il compito di tenere il Registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso.

Il Registro è uno degli strumenti che consentono al DPO di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile.

Come viene designato il DPO

La designazione del DPO compete sia al titolare che al responsabile del trattamento.

a) Casi in cui è obbligatoria la nomina²⁹

- il trattamento è effettuato da amministrazioni, enti pubblici e autorità giudiziarie nell'esercizio delle loro funzioni;
- le attività principali del titolare o del responsabile (quindi, soggetto privato) consistono in trattamenti che per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala (profilazione);
- trattamento di particolari categorie di dati³⁰ e di dati relativi a condanne penali³¹ su larga scala.

²⁹ Art. 37, par. 1, lett. a) – c).

b) Casi in cui NON è obbligatoria la nomina³²

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile della Protezione dei Dati non è obbligatoria.

Ad esempio, in relazione a trattamenti effettuati da:

- liberi professionisti operanti in forma individuale;
- agenti, rappresentanti e mediatori operanti non su larga scala;
- imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

In ogni caso, resta, comunque, raccomandata, anche alla luce del principio di "accountability" che permea il Regolamento, la designazione di tale figura, i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

2. QUALI CARATTERISTICHE DEVE AVERE IL DPO

Al Data Protection Officer non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi. Egli deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

Deve poter offrire, con professionalità e competenza, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena **indipendenza³³** e **autonomia**, senza ricevere istruzioni e riferendo direttamente ai vertici.

Il DPO deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti³⁴.

³³. Considerando 97, GDPR.

³⁴. Cfr. "Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato" del Garante privacy.

3. POSIZIONE DEL DPO ALL'INTERNO DELL'ORGANIZZAZIONE

L'indipendenza e l'autonomia del DPO si riflette nella sua posizione all'interno dell'organizzazione aziendale.

Pertanto, è necessario che:

- il titolare e il responsabile del trattamento assicurino che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti alla protezione dei dati personali;
- al DPO siano garantite le risorse necessarie per assolvere i compiti di cui all'art. 39 GDPR, accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;
- il DPO eserciti i propri compiti senza dipendere da istruzioni impartite dal titolare o dal responsabile del trattamento e, di conseguenza, non può essere rimosso o penalizzato per l'adempimento dei propri compiti.

Nello svolgimento dei propri compiti, inoltre, il DPO:

- riferisce direttamente al vertice gerarchico del titolare o del responsabile del trattamento;
- è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti;
- non può svolgere altri compiti e funzioni in conflitto di interessi;
- è il punto di contatto con gli interessati, per l'esercizio dei loro diritti o altra questione relativa al trattamento dei dati personali.

3.1 DPO E CONFLITTO DI INTERESSI

Il ruolo di DPO è compatibile con altri incarichi all'interno della medesima organizzazione, purché non sia in conflitto di interessi.

Proprio per scongiurare situazioni di conflitto di interessi, appare preferibile evitare di assegnare il ruolo di Data Protection Officer a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.).

L'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale) è da valutare caso per caso.

3.2 POSSIBILI CASI DI CONFLITTO DI INTERESSI

DPO Interno	DPO Esterno
<i>Direttore IT</i>	Rappresentante di organizzazione dei consumatori, i quali siano tipicamente soggetti interessati rispetto al trattamento del titolare e del responsabile.
<i>Direttore HR</i>	Avvocato che assista anche dipendenti o elementi della compagine societaria o controparti.
<i>Direttore Marketing</i>	Auditor esterno di una società nel contesto di processo di certificazione, non può essere anche DPO di quella società.

VIII

Il Data Breach

1. COSA SI INTENDE PER DATA BREACH

La violazione dei dati personali (Data Breach) è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita anche temporanea (**disponibilità** delle informazioni), la modifica (**integrità** delle informazioni), la divulgazione non autorizzata o l'accesso (**riservatezza** delle informazioni) ai dati personali trasmessi conservati o comunque trattati³⁵.

Dalla definizione data è chiaro che una violazione dei dati personali può avvenire anche per fatti che sono indipendenti dalla volontà di un soggetto. Occorre, quindi, valutare le condizioni oggettive con cui si verifica una violazione e non la provenienza dei comportamenti che l'hanno cagionata. Tuttalpiù, l'illiceità della condotta potrà avere delle conseguenze anche sul piano penale.

2. LA NOTIFICA DI UN DATA BREACH ALL'AUTORITÀ DI CONTROLLO³⁶

Il titolare del trattamento non è obbligato a notificare all'Autorità Garante ogni violazione dei dati personali, a meno che sia probabile che tale violazione presenti un rischio³⁷ per i diritti e le libertà delle persone fisiche³⁸.

In caso di notifica, questa andrà effettuata senza ingiustificato ritardo e, qualora possibile, entro 72 ore dal momento in cui il titolare del trattamento ne è venuto a conoscenza. A tale riguardo, il responsabile del trattamento deve informare il titolare delle violazioni di cui è venuto a conoscenza, senza ingiustificato ritardo.

Il termine di 72 ore non è tassativo, il titolare può notificare al Garante l'avvenuta violazione anche oltre tale termine, purché giustifichi i motivi del ritardo.

Come inviare la notifica al Garante

La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo protocollo@pec.gdpd.it oppure tramite posta elettronica ordinaria all'indirizzo protocollo@gdpd.it e deve essere **sottoscritta digitalmente** (con firma elettronica qualificata/firma digitale) ovvero con **firma autografa**. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia

³⁵ Cfr. art. 4, n. 12), GDPR.

³⁶ Art. 33, GDPR.

³⁷ Sulla valutazione del rischio a seguito di un data breach v. oltre, par. 5.

³⁸ L'art. 33, par. 1, GDPR, in realtà, è formulato in senso negativo "... il titolare del trattamento notifica la violazione all'autorità di controllo competente [...] a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche..."

del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura **"NOTIFICA VIOLAZIONE DATI PERSONALI"** e opzionalmente la denominazione del titolare del trattamento.

Azioni che il Garante può intraprendere a seguito di una segnalazione

Il Garante può prescrivere misure correttive³⁹ nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

3. CONTENUTO MINIMO DELLA NOTIFICA AL GARANTE

La notifica al Garante deve contenere almeno:

- a) la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) la descrizione delle probabili conseguenze della violazione dei dati personali;
- d) la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La notifica delle informazioni qui sopra riportate può avvenire anche per fasi successive qualora non sia possibile farlo contestualmente, purché, ancora una volta, senza ingiustificato ritardo

A prescindere dalla notifica al Garante o dalla comunicazione all'interessato⁴⁰, il titolare deve sempre documentare, nel c.d. Registro delle violazioni, qualsiasi violazione dei dati personali, comprese le circostanze in cui si sono manifestate, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Il Registro consente all'autorità di controllo di verificare il rispetto dell'art. 33, GDPR.

³⁹ Cfr. art. 58, par. 2, GDPR.

⁴⁰ V. paragrafo successivo.

4. LA COMUNICAZIONE ALL'INTERESSATO⁴¹

4.1 REQUISITI DELLA COMUNICAZIONE ALL'INTERESSATO

Se una violazione possa presentare un rischio **elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto a comunicarla agli interessati, senza giustificato ritardo.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno:

- il nome e i dati di contatto del DPO o altri soggetti dai quali poter ottenere ulteriori informazioni;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate per porvi rimedio e attenuarne i possibili effetti negativi.

4.2 QUANDO NON È RICHIESTA LA COMUNICAZIONE ALL'INTERESSATO⁴²

La comunicazione all'interessato non è richiesta nei seguenti casi:

- il titolare del trattamento aveva adottato misure tecniche ed organizzative adeguate per proteggere i dati personali oggetto della violazione (es. pseudonimizzazione o cifratura);
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Sul sito del Garante è disponibile il modello di notifica del data breach (<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501>)

⁴¹ Cfr. art. 34, GDPR.

⁴² Cfr. art. 34, par. 3, GDPR.

5. VALUTAZIONE DEL RISCHIO CONSEGUENTE A UN DATA BREACH

Al fine di valutare la gravità della violazione e quindi il grado di rischio per gli interessati, Il WP29 (ora EDPB)⁴³ suggerisce di prendere in considerazione:

- le caratteristiche particolari del titolare e degli interessati;
- il numero delle persone fisiche coinvolte;
- il tipo di violazione;
- la natura della violazione;
- il carattere sensibile e il volume dei dati personali violati;
- la facilità di identificazione delle persone fisiche interessate.

Per calcolare il rischio, le Linee Guida propongono una **formula elaborata dal'ENISA** – l'Agenzia della UE per la sicurezza delle reti e dell'informazione – che determina la gravità del data breach tenendo in considerazione tre fattori:

- contesto del trattamento -DPC (natura e volume dei dati violati, campo di attività del titolare, particolari categorie di interessati);
- facilità di identificazione -EI della persona a cui si riferiscono i dati violati (trascurabile, limitata, significativa, massima);
- circostanze della violazione -CB (perdita di riservatezza, integrità, disponibilità, dovuta a un evento accidentale oppure ad un'azione intenzionale).

A questi fattori viene attribuito un valore (fra quelli indicati in apposita tabella) tenuto conto della stima specifica del caso. Il grado di rischio è determinato dalla formula $DPC \times EI + CB$ (bassa, media, alta, molto alta).

A determinate soglie scatta la notifica e/o la comunicazione agli interessati.

Una interessante metodologia per la valutazione del rischio al fine di notificare la violazione dei dati al Garante è stata sviluppata dall'autorità di controllo spagnola (AEDP). Quest'ultima, con proprie linee guida⁴⁴, propone l'utilizzo di tre parametri, a cui sono assegnati dei punteggi:

- Il volume dei dati violati;
- La tipologia dei dati oggetto della violazione;
- L'impatto della violazione (intesa come grado di divulgazione dei dati violati).

⁴³ Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 adottate il 3 ottobre 2017 ed emendate il 6 febbraio 2018, disponibili all'indirizzo https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (consultate in data 06/11/2019).

⁴⁴ <https://www.aepd.es/media/guias/Guide-on-personal-data-breach.pdf>.

VIII | Il Data Breach

NUMERO DI ELEMENTI DI IDENTIFICAZIONE COMPLETI					
VOLUME	< 100	> 1.000	>=1.000 <=100.000	> 100.000	> 1.000.000
PUNTEGGIO	1	2	3	4	5

TIPI DI DATI TRATTATI (ai sensi del GDPR e della normativa speciale)		
TIPI DI DATI	DATI PERSONALI NON SENSIBILI	DATI PERSONALI SENSIBILI
PUNTEGGIO	1	2

IMPATTO (DIVULGAZIONE)					
LIVELLO IMPATTO	Zero	INTERNO (nell'ambito dell'organizzazione o del gruppo)	ESTERNO (fornitori o nella sfera di chi ha violato i sistemi)	PUBBLICO (accessibile su internet)	SCONOSCIUTO
PUNTEGGIO	2	4	6	8	10

La valutazione del rischio sarà compiuta sulla base della formula: Volume x (Tipologia x Impatto). Sulla base di determinati risultati occorrerà notificare e/o comunicare.

IX

*Gli amministratori
di Sistema*

1. QUAL È IL RUOLO DELL'AMMINISTRATORE DI SISTEMA?

L'amministratore di sistema è quella figura professionale che **abitualmente** si occupa della **gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali**, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali

Vi rientrano, quindi, tutti gli operatori di sistema nella misura in cui hanno possibilità di intervenire sui dati personali.

Restano esclusi quei soggetti che solo **occasionalmente** intervengono (es. per scopi di manutenzione a seguito di guasti o malfunzionamenti) sui sistemi di elaborazione e sui sistemi software.

2. MISURE DA ADOTTARE NELLA DESIGNAZIONE E GESTIONE DEGLI AMMINISTRATORI DI SISTEMA

Occorre prestare particolare attenzione nella scelta, nella gestione e nella verifica delle attività compiute dagli amministratori di sistema.

In proposito, il **provvedimento del Garante della protezione dei dati sugli amministratori di sistema**⁴⁵ provvede a individuare alcune misure organizzative che il titolare del trattamento deve adottare affinché l'amministratore di sistema svolga i propri compiti nel rispetto della normativa sulla protezione dei dati personali.

Fra queste:

- valutazione dell'esperienza, delle capacità e affidabilità del soggetto, sulla base di criteri equivalenti a quelli previsti dall'art. 28 GDPR per la designazione dei responsabili del trattamento;
- designazione **individuale**, con elencazione analitica (per settori o aree applicative) degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- un elenco degli amministratori di sistema contenente:
 - **gli estremi identificativi** delle persone fisiche amministratori di sistema (nome, cognome, funzione o area organizzativa di appartenenza)
 - l'elenco delle funzioni.

⁴⁵ Cfr. *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema del 27 novembre 2008 (modificato dal provvedimento del 25 giugno 2009).*

Queste informazioni devono essere riportate in un documento interno. I lavoratori devono conoscere l'identità degli amministratori di sistema, se sono trattati i loro dati. A tal fine, si provvederà a inserire i loro estremi identificativi nell'**informativa** o nel **disciplinare interno**⁴⁶. In alternativa, si possono anche utilizzare **strumenti di comunicazione interna** (es. intranet aziendale, ordini di servizio a circolazione interna o bollettini).

Amministratori in outsourcing.

In caso di funzioni di amministratore di sistema correlate alla sottoscrizione di un contratto di outsourcing con un fornitore di servizi informatici, il titolare o il responsabile del trattamento devono conservare gli estremi identificativi delle persone fisiche che svolgono le funzioni di amministratore di sistema.

3. VERIFICA DELLE ATTIVITÀ DEGLI AMMINISTRATORI DI SISTEMA

È necessario svolgere un controllo almeno annuale sulla conformità delle attività svolte dagli ADS rispetto ai compiti a loro assegnati.

In genere la verifica passa attraverso l'analisi dei log files, registrando gli accessi logici (autenticazione informatica) effettuati dagli ADS.

Quando registrare

- All'atto di accesso o tentativo di accesso o all'atto della disconnessione da parte dell'ADS, nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software che consentono, anche solo indirettamente, il trattamento di dati personali (cd. log in e log out).
- Non è richiesto il log di attività interattive o di transazioni (cd. audit log).

Cosa registrare

- I riferimenti temporali
- La descrizione dell'evento che li ha generati.

Devono essere conservati per un congruo periodo, **non inferiore a sei mesi**.

Una registrazione tipo potrà contenere:

- username utilizzato
- la data e l'ora dell'evento
- una descrizione dell'evento (log-in, log-out, tipo di errore, linea di comunicazione o terminale utilizzato).

Come registrare

⁴⁶ Cfr. *Linee guida del Garante sull'utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro* (Provvedimento n. 13 del 1° marzo 2007).

Le registrazioni devono avere caratteristiche di:

- **completezza;**
- **inalterabilità;**
- **possibilità di verifica della loro integrità.**

4. COME QUALIFICARE L'AMMINISTRATORE DI SISTEMA ALLA LUCE DEL GDPR

Amministratore di sistema in outsourcing

Quando il titolare del trattamento esternalizza un servizio ha la necessità di individuare quel soggetto che tratterà i dati personali per suo conto. L'art. 28 GDPR ha reso obbligatoria la nomina di un responsabile del trattamento che è sempre una figura esterna all'organizzazione del titolare e al quale quest'ultimo impartisce specifiche istruzioni sulle modalità di trattamento.

A ben vedere, l'amministratore di sistema in outsourcing è il responsabile del trattamento, ma con una importante specificazione; come ricordato al paragrafo 2, la designazione dell'amministratore di sistema è individuale, pertanto:

- se il responsabile del trattamento è una **persona fisica**, sarà egli stesso amministratore di sistema;
- se il responsabile del trattamento è una **persona giuridica**, allora dovrà designare una o più persone fisiche nell'ambito della propria organizzazione preposte alle funzioni di amministratori di sistema.

Amministratore di sistema interno all'organizzazione del titolare

Il titolare o il responsabile possono individuare specifiche persone fisiche, all'interno della propria organizzazione, da designare per l'adempimento di precisi compiti e funzioni e che opereranno sotto la loro autorità, trattando i dati personali secondo le modalità che titolare o responsabile

⁴⁷ Cfr. art. 2-quaterdecies, D.Lgs. 196/2003.

⁴⁸ Cfr. art. 29, GDPR.

riterranno più opportune⁴⁷.

Quindi, le persone fisiche autorizzate al trattamento e che già operano sotto l'autorità del titolare o del responsabile del trattamento, ma pur sempre sulla base delle istruzioni impartite dal titolare⁴⁸, possono essere designate per svolgere le funzioni proprie dell'amministratore di sistema.

5. SICUREZZA DEL TRATTAMENTO OPERATO DALL'AMMINISTRATORE DI SISTEMA

È all'amministratore di sistema che spetta porre in essere le misure indispensabili di sicurezza, come il backup e recovery dei dati, la custodia delle credenziali, la gestione dei sistemi di autenticazione e autorizzazione.

Per questo, accanto alle buone pratiche legate alla organizzazione e gestione della figura dell'amministratore di sistema viste nei precedenti paragrafi 2 e 3, è necessario che il titolare e il responsabile mettano in atto misure organizzative e tecniche adeguate per attenuare i rischi che inevitabilmente comporta l'esercizio delle attività di amministratore di sistema.

A tale scopo è importante tenere presenti il **Provvedimento del Garante del 27 novembre 2008** relativo a *“misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”*⁴⁹ e le best practice contenute nell'**allegato B al Codice per la protezione dei dati personali** – Disciplinare tecnico in materia di misure minime di sicurezza – che seppur abrogato dal D.Lgs. 101/2018 - può essere ancora oggi considerato un documento utile a orientare il titolare e il responsabile nell'attuazione e nel rispetto del principio di accountability rispetto alla gestione dei rischi connessi all'attività degli amministratori di sistema.

⁴⁹ G.U. n. 300 del 24 dicembre 2008 - Modificato in base al provvedimento del 25 giugno 2009.

X

*Controllo dei lavoratori
e videosorveglianza*

1. A QUALI CONDIZIONI IL DATORE DI LAVORO PUÒ TRATTARE I DATI DEI LAVORATORI

Nell'esercizio dei suoi poteri direttivi e di controllo, il datore di lavoro tratta le informazioni dei lavoratori anche al fine di effettuare la valutazione sul corretto adempimento della prestazione lavorativa, quasi sempre con la collaborazione di **personale addetto alla vigilanza** dell'attività lavorativa, previa comunicazione ai lavoratori dei loro nominativi con indicazione delle specifiche mansioni⁵⁰.

Il datore di lavoro è tenuto a trattare i dati dei lavoratori nel rispetto **dei principi di necessità, pertinenza e della più ampia trasparenza informativa**, servendosi degli strumenti messi a disposizione dalla legge e/o dai regolamenti interni, come l'informativa o il disciplinare interno.

L'utilizzo di un software che permetta il controllo del processo produttivo in tempo reale, ad esempio, sarebbe lecito nella misura in cui gli interessati al trattamento (i lavoratori) siano stati messi nelle condizioni di conoscere l'esistenza di uno strumento di monitoraggio, delle finalità del trattamento, mediante un'informativa e/o un disciplinare interno, diffusi attraverso mezzi di comunicazione interni (intranet aziendali, ordini di servizio, ecc.).

Non sono ammessi controlli che esulano dall'attività lavorativa ed in particolare quelli attinenti alla sfera personale del lavoratore. Così, il datore di lavoro non può condurre indagini sulle **opinioni politiche, religiose o sindacali del lavoratore** o su fatti che non rilevano ai fini della valutazione dell'attitudine professionale del lavoratore, sia ai fini dell'assunzione che nel corso dello svolgimento del rapporto di lavoro⁵¹.

2. PRESUPPOSTI PER IL CONTROLLO DEI LAVORATORI A DISTANZA

La norma cui fare riferimento per conoscere i presupposti del controllo a distanza dei lavoratori è l'art. 4, L. 300/1970, cui rinvia l'art. 114, Codice in materia di protezione dei dati personali⁵².

Esso prevede due modalità di controllo a distanza:

Mezzi di controllo rispetto ai quali il lavoratore è soggetto passivo (art. 4, c. 1)

⁵⁰ Cfr. art. 3, L. 300/1970 (Statuto dei Lavoratori).

⁵¹ Cfr. art. 8, L. 300/1970 e art. 10, D.Lgs. 276/2003, cui fa rinvio l'art. 113, D.Lgs 196/2003 (Codice Privacy).

Si tratta di strumenti che permettono anche la possibilità di un controllo a distanza dei lavoratori. Questi possono essere installati a condizione che:

- siano utilizzati esclusivamente per **esigenze organizzative e produttive**, per la **sicurezza del lavoro** e per la **tutela del patrimonio aziendale**;
- vi sia un previo **accordo collettivo** stipulato dalla **rappresentanza sindacale unitaria** o dalle **rappresentanze sindacali aziendali**.

In mancanza di tale accordo è possibile l'installazione:

- previo accordo collettivo stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale;
- in mancanza di accordo, previa **autorizzazione della sede territoriale dell'Ispettorato Nazionale del Lavoro (o della sede centrale dell'INL**, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali).

Sono esempi di mezzi di controllo di questo tipo:

- le **telecamere aziendali**. Le condizioni di cui all'art. 4, c.1 appena ricordate, devono essere rispettate anche se le telecamere non sono attive (telecamere "finte"), se è stato dato un preavviso ai lavoratori o il controllo sia discontinuo, perché esercitato in locali dove i lavoratori possono trovarsi solo occasionalmente⁵³;
- **tracciamento GPS**, salvo che il sistema sia installato in **adempimento di un obbligo di legge** (ad es. veicoli adibiti al trasporto di valori superiori a 1,5 milioni di euro) o sia utilizzato dal lavoratore per eseguire la prestazione (es consegna spedizioni)⁵⁴.

Mezzi di controllo rispetto ai quali il lavoratore è soggetto attivo (art. 4, c. 2)

Si tratta di strumenti che il lavoratore utilizza per eseguire la prestazione lavorativa o per la registrazione dei suoi accessi e delle presenze, per i quali non è richiesto un previo accordo sindacale.

Rientrano fra questi strumenti di controllo:

- badge di ingresso/uscita dalla sede aziendale;
- sistemi di accesso ad aree interne o riservate;
- strumenti di timbratura per certificare l'inizio della presa in carico di un'attività lavorativa presso una specifica area di produzione;
- supporti hardware (smartphone, tablet, PC aziendali);

⁵² L'art. 4, L. 300/1970 è stato da ultimo sostituito con D.Lgs. 151/2015 e modificato dal D.Lgs. 185/2016.

⁵³ Cfr. Nota del Ministero del Lavoro n.11241 del 1 giugno 2016.

⁵⁴ Cfr. Circolare n. 2/2016 dell'Ispettorato Nazionale del Lavoro.

- software e rete internet (sistemi operativi, browser, posta elettronica, applicazioni).

Qualora l'utilizzo di tali strumenti sia monitorato sistematicamente, in modo da consentire di fatto un controllo a distanza dei lavoratori, non sarebbe più rispettato il dettato dell'art. 4, c.2, della Legge n. 300/1970, costituendo una violazione dei diritti dei lavoratori. È il caso, ad esempio, della lettura sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto strettamente necessario per fornire il servizio e-mail o ancora la riproduzione e eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

Le informazioni raccolte ai sensi dei commi 1 e 2 del citato art. 4, possono essere usate a tutti i fini connessi al rapporto di lavoro, purché ne sia data al lavoratore adeguata informazione e nel rispetto di quanto previsto dal GDPR⁵⁵.

3. LA NAVIGAZIONE IN INTERNET DEL LAVORATORE

Le linee Guida del Garante per posta elettronica e internet del 1 marzo 2007⁵⁶, prescrivono al datore di lavoro l'adozione di misure organizzative e di tipo tecnologico volte a limitare l'uso improprio dei dati dei lavoratori, evitando controlli sistematici a distanza degli stessi lavoratori.

È di fondamentale importanza che dette misure, contenute in un disciplinare interno, siano redatte con un linguaggio semplice e chiaro e siano adeguatamente pubblicizzate e aggiornate periodicamente.

Per quanto riguarda in particolare la navigazione in internet, il datore di lavoro adotta opportune misure per prevenire controlli successivi sul lavoratore, che potrebbero determinare un trattamento di informazioni personali non pertinenti o idonee a rivelare le convinzioni religiose o filosofiche o di altro genere, le opinioni politiche, lo stato di salute o la vita sessuale del lavoratore. Il datore di lavoro può impedire che il lavoratore utilizzi impropriamente l'accesso a internet mediante:

- l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
- la configurazione di sistemi o l'utilizzo di filtri che prevenivano determinate operazioni;

⁵⁵ Cfr. art. 4, c. 3, L. 300/1970.

⁵⁶ Disponibili all'indirizzo <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522>

- il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
- l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
- la graduazione dei controlli.

4. L'USO DELLA POSTA ELETTRONICA DA PARTE DEL LAVORATORE

L'utilizzo della posta elettronica è in genere considerato riservato. Se il disciplinare interno non fosse chiaro su questo punto, il lavoratore potrebbe avere una legittima aspettativa a considerare confidenziale l'uso della posta elettronica.

Sarebbe opportuno che il datore di lavoro assicuri:

- la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali (info@ufficio.it);
- l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
- la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
- che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- la graduazione dei controlli.

5. LEGITTIMITÀ DEI CONTROLLI BASATI SU TECNICHE DI RICONOSCIMENTO BIOMETRICO

“I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche di una persona fisica che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici”. È questa la definizione che il GDPR⁵⁷ dà dei dati biometrici: le caratteristiche fisiche, fisiologiche o comportamentali degli interessati sono oggetto di un **procedimento tecnologico** (la scansione della retina, la registrazione della firma su un tablet) che permette di ricavare dei dati ulteriori, in grado di essere direttamente, univocamente e in modo tendenzialmente stabile nel tempo collegati a un individuo, consentendone o confermandone l’identificazione univoca.

I dati biometrici rientrano fra i cc.dd. dati appartenenti a categorie particolari di cui all’art. 9 GDPR, di cui è generalmente vietato il trattamento, salvo che non ricorrano le eccezioni previste al comma 2 dello stesso art. 9.

Fra queste, quella che ricorre nell’ambito di un rapporto di lavoro è rappresentata dal trattamento “necessario per assolvere gli obblighi e esercitare i diritti specifici del titolare del trattamento o dell’interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell’Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri...”⁵⁸.

Dal momento che l’Autorità Garante per la protezione dei dati personali non ha ancora adottato le misure di garanzia, ai sensi dell’art. 2-septies del D.Lgs. n. 196/2003, è opportuno fare riferimento al **Provvedimento generale prescrittivo in tema di biometria**, adottato dallo stesso Garante il 12 novembre 2014, e alle **relative Linee-guida in materia di riconoscimento biometrico e firma grafometrica** (Allegato A al provvedimento), per individuare le misure di sicurezza di carattere tecnico, organizzativo e procedurale idonee a mantenere alti livelli di sicurezza a garanzia degli interessati.

Resta in ogni caso in capo ai titolari e ai responsabili, in virtù del principio di accountability, l’onere di adottare tutte le misure necessarie a mitigare i rischi per i diritti, le libertà e la dignità dei lavoratori.

⁵⁷ Cfr. art. 4, n. 14), GDPR.

⁵⁸ Cfr. art. 9, c. 2, lett. b), GDPR.

⁵⁹ Cfr. art. 35, GDPR.

Non è esclusa, infine, la necessità di procedere ad una **valutazione di impatto dei dati** (Data Protection Impact Assessment – DPIA)⁵⁹, nel caso di controlli a distanza dei lavoratori basati su sistemi tecnologici (fra i quali le tecniche di riconoscimento biometrico, la videosorveglianza e la geolocalizzazione), tenendo conto, in particolare, del **volume di dati**, della **durata**, o della **persistenza dell'attività di trattamento**.

XII

*Ulteriori approfondimenti
in materia di protezione
dei dati personali*

1. NELL'AMBITO DELLE ATTIVITÀ DI MARKETING DIRETTO, IN CHE MODO IL TITOLARE DIMOSTRA CHE NON È NECESSARIO IL CONSENSO DEGLI INTERESSATI?

Nell'ambito del marketing diretto, il fornitore contatta, in genere via e-mail, il cliente per proporgli la vendita di prodotti o servizi in linea con quanto abbia già acquistato in passato.

L'art. 130, comma 4, del Codice in materia di protezione dei dati personali permette al titolare del trattamento di utilizzare gli indirizzi di posta elettronica, forniti dagli interessati al momento dell'acquisto di beni o servizi offerti dal medesimo titolare, al fine di vendere altri beni o servizi analoghi, senza richiedere il consenso dell'interessato, così come sarebbe prescritto dal comma 1 dello stesso art. 130.

Il titolare, attraverso il Registro dei trattamenti di cui all'art. 30, GDPR, dimostra di possedere i dati raccolti al momento della prima vendita di beni o servizi, così da poter provare la sussistenza dell'analogia fra quei beni o servizi venduti e quelli proposti successivamente agli stessi clienti mediante posta elettronica e la mancata opposizione dell'interessato al momento della raccolta dei suoi dati personali a ricevere comunicazioni via e-mail in un contesto di marketing diretto.

Si rimanda al [**Cap. II, par. 2**](#) per ulteriori chiarimenti.

2. LE SOCIETÀ O GLI STUDI DI CONSULENZA REGOLATORIA HANNO L'OBBLIGO DI NOMINARE UN DPO E DELLA TENUTA DEL REGISTRO DEI TRATTAMENTI?

Qualora le società o gli studi di consulenza regolatoria trattino su larga scala dati personali riconducibili alle categorie di cui all'art. 9, GDPR (in particolare dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) saranno certamente tenute a nominare un DPO.

Quanto all'obbligo della tenuta del Registro dei trattamenti, sia che operi in quanto titolare o responsabile del trattamento, la società o lo studio di consulenza regolatoria dovrà predisporre il predetto Registro, dal momento che, come chiarito al [**Cap. IV, par. 2**](#), la circostanza che un titolare o un responsabile effettui un trattamento non occasionale, che non presenti un rischio (anche non elevato) per i diritti e le libertà degli interessati è alquanto

remota.

Inoltre, le società regolatorie trattano con buona probabilità dati personali appartenenti ai tipi di cui all'art. 9, GDPR, per i quali è previsto l'obbligo della tenuta del Registro dei trattamenti qualunque sia la dimensione dell'organizzazione.

Infine, si ricorda che, al di fuori dei casi di tenuta obbligatoria del Registro, l'Autorità garante per la protezione dei dati personali ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

L'argomento è ampiamente trattato al [Cap. IV](#).

3. È OBBLIGATORIO NOMINARE INDIVIDUALMENTE LE PERSONE AUTORIZZATE AL TRATTAMENTO?

Non sussiste un obbligo di nomina individuale degli autorizzati al trattamento. Gli stessi possono essere individuati sulla base di categorie omogenee, ciascuna con proprie funzioni contenute in appositi mansionari.

Gli autorizzati al trattamento chiamati a svolgere funzioni di amministratori di sistema, devono essere designati individualmente (si v. [Cap. IX, par. 2](#)).

4. NELL'AMBITO DELLE ATTIVITÀ SVOLTE IN QUALITÀ DI CTU (CONSULENTE TECNICO D'UFFICIO), È NECESSARIO RENDERE L'INFORMATIVA ALLE PARTI?

Com'è noto i consulenti tecnici e i periti ausiliari del Giudice e del Pubblico Ministero coadiuvano e assistono l'autorità giudiziaria nello svolgimento delle proprie funzioni, quando ciò si rende necessario per compiere atti o esprimere valutazioni che richiedono particolari e specifiche competenze tecniche.

Ne deriva che l'attività svolta dai consulenti tecnici e dai periti è strettamente connessa e integrata con l'attività giurisdizionale, **di cui mutua i compiti e le finalità istituzionali**.

La conseguenza di quanto appena chiarito è che alle attività dei periti e dei consulenti tecnici si applicano i limiti e le condizioni previsti dal GDPR e dal

Codice in materia di protezione dei dati personali riguardo al trattamento dei dati personali da parte delle autorità giudiziarie, nell'esercizio delle loro funzioni.

In particolare, l'art. 2-duodecies, c. 1, D.Lgs. n. 196/2003, introdotto dal D.Lgs.101/2018, in attuazione di quanto previsto all'art. 23, par. 1, lett. f), GDPR, prevede che i "trattamenti di dati personali effettuati per **ragioni di giustizia**⁶⁰ nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, **i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti**, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento". Ai consulenti e periti, pertanto, si applicano le disposizioni di legge o di regolamento che regolano gli specifici procedimenti nei quali sono chiamati a svolgere la propria attività e non trova applicazione la disposizione di cui all'art. 13, GDPR, in materia di informativa.

Per una più ampia comprensione degli obblighi e dei limiti cui sono soggetti i consulenti tecnici si rimanda alla lettura delle **Linee guida del Garante per la protezione dei dati personali in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero** del 26 giugno 2008⁶¹, tenendo conto delle modifiche intervenute con l'entrata in vigore del GDPR e del D.Lgs. 101/2018.

⁶⁰ Cfr. art 2-duodecies, c. 4, per la definizione di "ragioni di giustizia", ai sensi del quale "a<i>fini del presente articolo si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività' ispettive su uffici giudiziari. Le ragioni di iustizia non ricorrono per l'ordinaria attività' amministrativo-gestionale di personale, mezzi o strutture, quando non e' pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti".

⁶¹ <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1534086>.

5. GLI OBBLIGHI ASSOLTI AI SENSI DEL GDPR PER ATTIVITÀ SVOLTE IN QUALITÀ DI TITOLARE DEL TRATTAMENTO A FAVORE DI UN CLIENTE, IN VIRTÙ DI UN CONTRATTO DI CONSULENZA, RESTANO FERMI ANCHE IN CASO DI INCARICO DI CTU ASSEGNATO DALL'AUTORITÀ GIUDIZIARIA, IN UN PROCEDIMENTO IN CUI È PARTE LO STESSO CLIENTE?

Occorre tenere distinte le due attività. Mentre la prima attiene all'esecuzione di un contratto di consulenza fra privati, per la quale valgono i principi e le norme contenute nel GDPR e nel Codice in materia di protezione dei dati personali, la seconda, come già ampiamente illustrato al punto 4, a cui si rinvia, riguarda lo svolgimento di una diversa e distinta funzione, nell'ambito della quale il trattamento dei dati personali è svolto per ragioni di giustizia.

6. COSA SUCCEDDE SE UN CLIENTE CHIEDE ESPRESSAMENTE L'ANONIMATO?

Nella maggior parte dei casi, fornire i propri dati personali è necessario per dar corso all'esecuzione del contratto per i quali tali dati sono richiesti.

Il titolare del trattamento è comunque obbligato a indicare le conseguenze del mancato conferimento dei dati personali.

Pertanto, il cliente sarà libero di non fornire i propri dati personali, ma ciò potrebbe comportare l'impossibilità di eseguire il contratto che vuole concludere.

Quanto all'esercizio dei diritti dell'interessato per i dati personali già forniti si rinvia a quanto riportato al **Cap. I, par. 3.**

7. ALCUNI ESEMPI DI LEGITTIMI INTERESSI QUALI BASE GIURIDICA DEL TRATTAMENTO

In base al Considerando 47 GDPR, *"...i legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che..."* siano **sufficientemente articolati** da

permettere il **test di bilanciamento** (da effettuare caso per caso) con gli interessi o i diritti fondamentali dell'interessato, soprattutto nel caso in cui quest'ultimo sia un minore e **reale e attuale**, cioè corrispondano ad un beneficio atteso in un futuro prossimo.

Tra i legittimi interessi del titolare si possono menzionare:

- il trattamento dei dati per finalità di marketing diretto⁶²;
- l'elaborazione dei dati in funzione della protezione contro le frodi;
- il trasferimento di dati personali tra organizzazioni appartenenti al medesimo gruppo imprenditoriale⁶³;



Per una più agevole comprensione del presente vademecum, consulta il testo del Regolamento (UE) n. 2016/679, arricchito con i riferimenti ai Considerando.

⁶² Cfr. Cap I, par. 2.

⁶³ Cfr. Considerando n. 48 GDPR.

Camera di commercio di Milano Monza Brianza Lodi

SEDE LEGALE

Via Meravigli, 9/b
20123 Milano
Tel +39 02.8515.1
www.milomb.camcom.it