Lucca Holding S.p.a.

Linee guida in materia di *privacy*

Parte generale

I. Premessa

Le presenti linee guida predisposte da Lucca Holding S.p.a. hanno lo scopo di supportare la stessa capogruppo e le società partecipate nella adozione degli adeguamenti imposti dall'entrata in vigore del regolamento 2016/679, denominato "*General Data Protection Regulation*" ("**GDPR**" o il "**Regolamento**").

Resta inteso che il presente documento rappresenta una linea guida di indirizzo generale con alcuni consigli pratici, mentre per l'adeguamento al Regolamento, dovranno provvedere le singole società del gruppo sulla base delle proprie singole specificità.

*

II.- I principi generali

Prima di entrare nel merito delle condotte da porre in essere pare opportuno soffermarsi brevemente sui principi fondamentali che informano il GDPR, contenuti all'art. 5 del GDPR.

Si tratta, in particolare, del:

a) principio di liceità, correttezza e trasparenza;
b) principio di limitazione della finalità;
c) principio di minimizzazione dei dati;
d) principio di esattezza;
e) principio di limitazione della conservazione;
f) principio di integrità e riservatezza (*confidentiality*);
e) principio di responsabilizzazione (*accountability*).

II.1.- Il principio di liceità, correttezza e trasparenza

Il primo principio stabilisce che i dati devono essere trattati «*in modo lecito, corretto e trasparente nei confronti dell'interessato*».

Si tratta dunque di un principio che in realtà contiene tre sotto-principi: il primo, generalissimo, è quello della liceità.

Si tratta di un principio apparentemente ridondante, ma il cui scopo in realtà è assicurare che il trattamento di dati non solo sia rispettoso delle disposizioni del Regolamento ma in generale delle carte sovranazionali dei diritti (CEDU, Carta dei diritti Fondamentali dell'UE, Costituzioni nazionali) e delle altre norme di legge (anche penali, amministrative e di ordine pubblico dei vari Stati membri), nell'ambito di un corretto bilanciamento tra interessi del titolare del trattamento e interessi dei soggetti interessati.

Una diretta specificazione di tale principio proviene dall'art. 6, che impone una base giuridica per ogni trattamento di dati, sia questa il consenso dell'interessato, un interesse legittimo, l'esercizio di un diritto o un interesse pubblico.

Il secondo sotto-principio è quello della correttezza: tale principio va oltre al principio formalistico della liceità. Il concetto di "correttezza" (o di "lealtà", come nella precedente Direttiva), infatti, richiama la nozione civilistica di correttezza e buona fede tipica del diritto delle obbligazioni e del diritto dei contratti.

Esso non si sostanzia nel mero divieto di violare specifiche disposizioni normative, ma nel divieto di abusare della propria posizione a danno dei legittimi interessi della controparte. Nell'ambito del trattamento di dati personali, dunque, ciò si traduce nel divieto per il titolare (e il responsabile) di trattare i dati personali in un modo che, seppur non direttamente in violazione di norme di legge, abusi della buona fede dei soggetti interessati e dunque sia contrario a correttezza e buona fede.

Il terzo sotto-principio è una delle maggiori novità rispetto alla normativa previgente: la trasparenza. Il principio di trasparenza è ispiratore di una serie di innovazioni presenti nel Regolamento: ne sono un esempio i maggiori requisiti di chiarezza negli obblighi informativi del titolare del trattamento (artt. 13 e 14) e la più ampia portata del diritto d'accesso ai dati personali (art. 15), anche in tema di comprensibilità degli algoritmi di profilazione. Anche i più specifici e stringenti requisiti in materia di "consenso" al trattamento dei dati personali (art. 7) rispondono ad un più ampio principio di trasparenza del trattamento.

I tre suesposti sotto-principi sono enunciati congiuntamente poiché rispondono tutti alla generale *ratio* di evitare trattamenti di dati personali abusivi, opachi, sleali o comunque illeciti.

II.2.- Il principio di limitazione della finalità

Il principio di limitazione della finalità prevede che i dati siano «*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*» (art. 5(1), lett. b)).

Si tratta di uno dei principi più importanti dell'intero Regolamento a sua volta a fondamento di altri principi, come quello di minimizzazione, di esattezza, o di limitazione della conservazione, ed espressivo a sua volta del principio di trasparenza.

Il principio di limitazione della finalità riguarda due diversi momenti del trattamento dei dati: la raccolta dei dati e il successivo trattamento.

Riguardo alla raccolta, essa deve essere effettuata per finalità:

a) determinate al momento stesso della raccolta e dunque previste a priori;
b) esplicite, dunque rese note sin da subito al soggetto interessato;
c) legittime, dunque tutelate o comunque permesse nel nostro ordinamento.

Riguardo al successivo trattamento, esso deve essere rispettoso delle finalità inizialmente determinate ed esplicitate al momento della raccolta.

Ciò vuol dire che è vietato trattare i dati per finalità secondarie, diverse da quelle per cui i dati erano stati inizialmente raccolti. Tale divieto, tuttavia, appare particolarmente problematico nel mondo dei Big Data, laddove il grande potenziale predittivo (e i relativi possibili usi) dei dati personali non è noto al momento della raccolta.

Per ovviare a tale problema, l'art. 6 permette gli usi secondari dei dati, nella misura in cui questi siano compatibili alle finalità iniziali (in base ad una serie di

indici, come il nesso tra la finalità iniziale e quella secondaria, il contesto, la natura dei dati, le possibili conseguenze di usi secondari e eventuali garanzie adeguate prestate).

Peraltro, proprio in virtù del giudizio di compatibilità qui citato, lo stesso articolo 5(1), lett. b), per evitare di limitare troppo la ricerca e la libertà di espressione stabilisce che «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 [e dunque purché abbia garanzie adeguate, come la pseudonimizzazione], considerato incompatibile con le finalità iniziali».

II.4.- Il principio di minimizzazione dei dati

Il principio di minimizzazione dei dati è una diretta conseguenza del principio di finalità sopraesposto, esso prevede che i dati raccolti debbano essere «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*» (art. 5(1), lett. c)).

In altri termini, una volta determinate le finalità (esplicite e legittime del trattamento) i dati personali in concreto raccolti non devono essere superflui, inutili o sovrabbondanti rispetto alle stesse finalità.

È stato in passato anche denominato "principio di necessità".

II.5.- Il principio di esattezza

Il principio di esattezza, prevede che i dati trattati debbano essere «*esatti e, se necessario, aggiornati*» (art. 5(1), lett. d)). Nell'interesse tanto dell'interessato quanto del titolare e del responsabile del trattamento è richiesto che i dati raccolti siano accurati e non rappresentino falsamente la realtà, ciò anche in ossequio ad un diritto all'identità personale (diritto a non essere falsamente rappresentati) del soggetto interessato del trattamento.

Una diretta conseguenza è che «*devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*».

Pertanto la rettifica (art. 16) e l'eventuale cancellazione dei dati (art. 17) non sono soltanto diritti dei soggetti, ma (qualora necessario) sono anche obblighi generali per i titolari del trattamento in ossequio al principio di esattezza.

L'esattezza riguarda il momento statico del trattamento dei dati, mentre l'aggiornamento dei dati stessi riguarda il momento dinamico del trattamento (necessario solo qualora il trattamento sia destinato a durare nel tempo o si basi su dati di per sé suscettibili di variazione nel tempo).

II.6.- Il principio di limitazione della conservazione

Il principio di limitazione della conservazione obbliga a conservare i dati personali «*in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*».

In altri termini, una volta conseguite le finalità del trattamento, i dati vanno eliminati o anonimizzati. Come appare chiaro, dunque, anche questo principio è una diretta emanazione del principio di finalità. Peraltro, anche in questo caso il

Regolamento ha voluto limitare l'impatto di tale limitazione sulla ricerca e sulle finalità pubbliche, pertanto l'art. 5(1), lett. e) chiarisce che «*i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato*», come ad esempio la pseudonimizzazione o la cifratura.

II.7.- Il principio di integrità e riservatezza

Il principio di integrità e riservatezza è una novità del Regolamento. Esso prevede che i dati siano «trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali». Tale principio è espresso in inglese col termine "*confidentiality*" e stabilisce la necessità per ogni trattamento di assumere adeguate misure tecnologiche od organizzative a garanzia della sicurezza e della protezione dei dati. Questo principio, in altri termini, introduce il concetto di *cybersecurity* e di "*security by design*" tra i pilastri della tutela dei dati personali.

È un principio intimamente connesso col principio di esattezza, tuttavia questo si concentra sui mezzi per evitare alterazioni dolose o colpose che ledano l'accuratezza di un trattamento di dati personali.

II.7.- Il principio di accountability

Il principio di "*accountability*" (responsabilizzazione) è un corollario di tutti i suesposti principi.

L'art. 5(1) afferma che il titolare del trattamento (e non, ad esempio, anche il responsabile) è competente per il rispetto di tutti i principi esposti all'art. 5 e deve essere "in grado di comprovarlo".

Il concetto di *accountability* è di difficile traduzione nella lingua italiana. Il Regolamento prova per la prima volta a tradurlo col termine di "responsabilizzazione".

La ratio di tale principio è rendere efficacemente applicabili i principi suesposti attraverso la responsabilizzazione di un unico soggetto (il titolare del trattamento) a cui ci si può facilmente e direttamente rivolgere al fine di chiedere la prova del rispetto dei principi del trattamento di cui all'art. 5.

Il principio di *accountability* nell'ambito del Regolamento si sostanzia in una serie di obblighi od oneri, come la produzione di un documento per la valutazione dell'impatto del trattamento dei dati (art. 35); l'obbligo di tenere un registro dei trattamenti (art. 30); oltre alle previsioni in materia di certificazioni, sigilli (art. 42) e codici di condotta (art. 40).

*

III.- La legittimità del trattamento ai sensi dell'art. 6

Il consenso costituisce il fondamento legale della legittimità del trattamento ai sensi dell'art. 6 lett. a).

Nel regolamento sono stati introdotti, tuttavia, requisiti più stringenti rispetto all'acquisizione dello stesso che incidono sui meccanismi di raccolta:

- trattamento in esecuzione di un contratto con l'interessato (art. 6, lett. b);
- trattamento al fine di ottemperare ad un obbligo legale secondo le norme dell'Unione Europea o di uno stato membro. La norma circoscrive l'effettività degli obblighi giuridici alla normativa europea o nazionale di uno stato membro (art. 6, lett. c).
- trattamento finalizzato alla salvaguardia di un interesse vitale dell'interessato o di altra persona fisica: il considerando 46 specifica che la base giuridica possa essere rinvenuta rispetto al trattamento necessario a fini umanitari, come in caso di necessità di tenere sotto controllo l'evoluzione e la diffusione di epidemie, oppure in caso di catastrofi (art. 6, lett. d).
- trattamento eseguito per un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, lett. e).[1]
- trattamento finalizzato al perseguimento di un interesse legittimo del titolare del trattamento o di terzi, purché non prevalga la tutela di diritti o libertà fondamentali dell'interessato (art. 6 lett. f).

L'art. 6, comma 2, del Regolamento attribuisce, in ogni caso, agli Stati membri il potere di mantenere o introdurre misure più specifiche relativamente al trattamento connesso con la libertà di espressione e di informazione (disciplinato dall'art. 85), con l'accesso del pubblico ai documenti ufficiali (art. 86), con il numero di identificazione nazionale (art. 87), con il rapporto di lavoro (art. 88); con le finalità di archiviazione nel pubblico interesse, ricerca scientifica o storica o dati statistici (art. 89); con gli obblighi di segretezza (art. 90); con le chiese e associazioni religiose (art. 91); gli Stati membri sono altresì autorizzati ad introdurre basi legali supplementari al fine di perseguire obiettivi connessi con la legislazione nazionale e con l'espletamento dell'interesse pubblico.

III.1.- Liceità del trattamento di particolari categorie di dati

L'art. 9 del Regolamento stabilisce il divieto di trattare i dati «*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*», ovvero quei dati personali cc.dd. sensibili (rispetto ai diritti e alle libertà

[1] In tale ultimo caso, occorre conservare tutta la documentazione comprovante il corretto bilanciamento dei diritti dell'interessato. Il limite di cui alla lettera f) non si applica in caso di autorità pubbliche nell'esercizio delle proprie funzioni. A tal proposito, i considerando 47, 48, 49 e 50 del Regolamento enucleano alcuni interessi legittimi capaci di fungere da base per un legittimo trattamento dei dati. Tra questi, il Regolamento si riferisce, in particolare, alla prevenzione delle frodi e alle finalità di marketing diretto; oppure alla trasmissione dei dati all'interno di un gruppo imprenditoriale a fini amministrativi interni, purché (eventualmente) nel rispetto della normativa sul trasferimento dei dati verso Paesi terzi.
In tale prospettiva, il trattamento dei dati relativi al traffico può assumere il carattere di interesse legittimo al fine di «*garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi*».

fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali, a norma del considerando 51), salvo il verificarsi di alcune condizioni.

Rispetto alla Direttiva 95/46/CE, il Regolamento introduce alcune ipotesi supplementari di trattamento. Il consenso dell'interessato resta, in ogni caso, la primaria base giuridica a giustificazione del trattamento anche delle predette categorie di dati (sinteticamente enucleabili in dati cc.dd. sensibili, biometrici, sanitari).

In aggiunta al consenso, l'art. 9 individua ulteriori trattamenti leciti:

- nel contesto del diritto del lavoro o della normativa concernente la sicurezza e previdenza sociale (lett. b);
- in ragione della necessità di tutelare un interesse vitale della persona o di un terzo incapace (lett. c);
- nel corso di attività di beneficienza, enti no-profit in relazione ai propri membri, ex membri (e tale aggiunta costituisce la novità rispetto al precedente assetto), o persone connesse a tali obiettivi (lett. d);
- qualora l'interessato abbia manifestamente reso pubblici i suddetti dati (lett. e);
- se finalizzato ad instaurare e/o difendersi in procedimenti, oppure sia eseguito dall'autorità giudiziaria nell'esercizio della propria funzione giurisdizionale (lett. f);
- se necessario per ragioni sostanziali di interesse pubblico (lett. g) o di medicina preventiva e/o del lavoro (lett. h) o al fine di accertare la capacità lavorativa dei dipendenti e la gestione dei servizi relativi al sistema sanitario o della sicurezza sociale (lett. i), solo se trattati da o sotto la responsabilità di un professionista sottoposto a segreto professionale.
- se necessario per interesse pubblico, storico, scientifico o di ricerca (lett. j).

Parimenti, ogni Stato membro può introdurre o mantenere condizioni e/o limitazioni al trattamento di dati genetici, biometrici o sanitari.

A chiusura dei requisiti di liceità di un trattamento si pone la norma di cui all'art. 6, comma 4, del Regolamento con cui è disciplinato il trattamento – eseguito senza consenso dell'interessato, né in osservanza di una specifica disposizione di legge dell'UE o dello Stato membro – per una finalità diversa da quella per la quale sono stati raccolti. In tal caso, il titolare deve operare una valutazione di compatibilità del trattamento, considerando – in particolare – ogni nesso tra le diverse finalità, la relazione con l'interessato, le conseguenze sull'interessato, anche in ragione della categoria dei dati, nonché la sussistenza di garanzie adeguate (pseudonimizzazione e cifratura) degli stessi.

III.2.- Le categorie sensibili e le ragioni di una tutela specifica

Tutti i dati che riguardano persone identificate ed identificabili godono della particolare protezione fornita dal Regolamento.

Tuttavia, tra di essi, alcune categorie (i c.d. "dati sensibili", o "categorie particolari di dati") godono di una speciale protezione da parte del Regolamento.

Infatti, come già emerso sopra ad esempio c'è una maggiore limitazione alla liceità di trattamento di tali dati (art. 9); inoltre, la presenza di dati sensibili obbliga a specifiche misure di protezione ed al consenso esplicito del soggetto; peraltro se i dati sensibili sono trattati su larga scala è sempre necessario un DPO (art. 36); c'è un obbligo di registri di attività di trattamento anche per i titolari con meno di 250 dipendenti che ne sarebbero in generale esenti (art. 30).

In generale, l'art. 9 delinea la figura di "categorie particolari di dati personali". Tali dati non costituiscono una categoria unitaria (come era invece per il Codice in materia di protezione dei dati personali), com'è dimostrato anche dalla mancanza di una definizione unitaria di tali dati all'art. 4.

L'art. 9 include da un lato «*dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale*», dall'altro lato altre categorie (queste sì unitarie) di dati definite all'art. 4 del GPDR: "dati genetici" (art. 4, n. 13), "dati biometrici intesi a identificare in modo univoco una persona fisica" (art. 4, n. 14), "dati relativi alla salute" (art. 4, n. 15) o "dati relativi alla vita sessuale o all'orientamento sessuale della persona".

Si tratta dunque di dati personali che meritano una specifica protezione perché, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, «*dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali*» (considerando 51).

In particolare, il maggiore rischio è quello della discriminazione. Infatti, come emerge dal considerando 71, il Regolamento si preoccupa che i dati siano trattati con modalità che tengano conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impediscano tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportino misure aventi tali effetti.

III.3.- I dati biometrici e il caso delle fotografie

Per quanto riguarda i dati biometrici così intesi, sorge il problema delle immagini facciali e dunque del trattamento delle fotografie.

Il considerando 51 chiarisce che il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica.

Rientrano nell'ipotesi descritta dal considerando 51, ad esempio, gli smartphone capaci di identificare i soggetti in base ai volti ritratti nelle fotografie. Un caso analogo è stato oggetto di una pronuncia del garante per i dati personali italiano (provv. n. 360/2015, in cui il Garante ha richiesto che per l'uso del software utilizzato da Costa Crociera per identificare i volti dei clienti nelle foto al fine di agevolare la vendita personalizzata delle foto scattate durante la crociera fossero presenti appositi cartelli di segnalazione e fossero distrutti i dati identificativi

dei volti appena non più necessari alle finalità).

In realtà, già prima del Regolamento, le fotografie del volto, in quanto rivelatrici dell'origine etnica di un soggetto (colore della pelle, tratti somatici), potevano considerarsi dati sensibili.

III.4.- I dati relativi alla salute

Un ultimo riferimento appare necessario per i dati relativi alla salute. Innanzitutto è bene distinguere tra "dati relativi alla salute" e "usi sanitari di dati personali".

Infatti, nel primo caso si tratta di una categoria speciale di dati (a prescindere dal loro trattamento), nel secondo caso invece si tratta di qualsiasi dato personale che venga trattato per finalità sanitarie (l'art. 9(2), lett. h e i, Regolamento prevede come casi di liceità per il trattamento di tutte le categorie particolari di dati personali i casi di "diagnosi, assistenza o terapia sanitaria" e di "motivi di interesse pubblico nel settore della sanità pubblica").

Quanto alla categoria di "dati relativi alla salute", l'art. 4 al n. 15 li definisce come dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Inoltre, il considerando 35 chiarisce che nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso.

Questi, in particolare, comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria come un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro (considerando 35).

*

IV.- La valida acquisizione del consenso

Come osservato sopra, il consenso costituisce la base prioritaria della liceità del trattamento dei dati personali, nonché dei dati appartenenti a particolari categorie, per semplicità enucleati in dati sensibili, biometrici e sanitari.

L'art. 4 del Regolamento definisce consenso qualsiasi manifestazione di volontà dell'interessato che sia espressa liberamente, che sia specifica rispetto ad un determinato trattamento, che sia informata circa le caratteristiche del trattamento ed inequivocabile in ordine all'assenso.

In particolare, la manifestazione deve essere eseguita mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. L'art. 2, lett. h), della previgente Direttiva 95/46/CE definiva consenso dell'interessato «*qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento*». Ciò determinava che in linea di principio non esistessero limiti di forma, essendo considerata valida "qualsiasi manifestazione".

Corollario della specificità del consenso è costituito dalle caratteristiche raccomandate per l'informativa: quest'ultima deve essere qualitativamente adeguata (rispetto al linguaggio utilizzato, ad esempio) e accessibile per gli interessati anche da un punto di vista grafico.

Il considerando 32 – nel ribadire le caratteristiche del consenso (definendolo un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano) – esclude che il silenzio possa costituire una accettazione valida al trattamento.

La fase di acquisizione del consenso, pertanto, pur essendo caratterizzata dalla libertà delle forme, necessita di una condotta positiva da parte dell'interessato.

Quest'ultimo può esprimersi per scritto, verbalmente, "spicchettando" una casella in una pagina web, attraverso una dichiarazione o altra condotta che indichi in un determinato contesto l'accettazione del trattamento dei dati personali, anche attraverso la scelta di impostazioni tecniche in una particolare applicazione.

Sono escluse l'adesione passiva con caselle pre-selezionate, l'inattività e il silenzio.

Ai sensi dell'art. 7, comma 1, del Regolamento e il considerando 42, occorre obbligatoriamente che l'accettazione del trattamento da parte dell'interessato consenta al titolare di "dimostrare" la corretta acquisizione del consenso, ciò costituisce una novità rispetto all'assetto normativo precedente.

L'art. 7, comma 2, stabilisce, inoltre, che se il consenso sia manifestato in forma scritta nel contesto di altre questioni, la richiesta di accettazione al trattamento dei dati personali debba essere presentata in modo distinto, in una forma intellegibile e facilmente accessibile: il consenso al trattamento non può, pertanto, essere acquisito nell'ambito di altre condizioni contrattuali.

L'art. 7, comma 3, del Regolamento disciplina il diritto dell'interessato a revocare il consenso prestato, obbligando altresì i titolari del trattamento a semplificare le modalità di esercizio del diritto di revoca.

La revoca può essere prestata in qualsiasi momento e si esprime attraverso modalità di pari semplicità rispetto a quelle con cui è stato manifestato il consenso al trattamento: se il consenso è stato prestato "spicchettando" una casella, l'interessato deve essere messo nelle condizioni di revocarlo attraverso la "spicchettatura" di una casella.

La revoca non è retroattiva: non pregiudica la legittimità del trattamento effettuato sulla base del consenso previamente espresso.

Il diritto e le modalità di esercizio della revoca costituiscono parte integrante dell'informativa dell'interessato (su cui ved. cap.2, sez. 2. "Diritto di revocare il consenso").

*

V.- I diritti dell'interessato: quadro generale

Una delle sezioni più importanti del Regolamento è quella che riguarda i diritti dell'interessato (artt. 15-22). Si tratta della parte che più richiede uno sforzo organizzativo e tecnologico da parte del titolare del trattamento e dunque un relativo lavoro di controllo e consulenza da parte del DPO. Peraltro, è tra i diritti dell'interessato che si registrano le maggiori novità del Regolamento rispetto alla previgente Direttiva 95/46.

Nel complesso i diritti dell'interessato rispetto al trattamento dei suoi dati personali sono i seguenti:

1. diritto di revocare il consenso (art.7(3));
2. diritto a ricevere informazioni (artt. 13 e 14);
3. diritto di accesso (art. 15);
4. diritto alla rettifica (art. 16);
5. diritto alla cancellazione ("diritto all'oblio") (art. 17);
6. diritto di limitazione di trattamento (art. 18);
7. diritto alla portabilità dei dati (art. 20);
8. diritto di opposizione (art. 21);
9. diritto a non essere soggetti a profilazione automatizzata (art. 22).

Come indirizzo generale per garantire l'esercizio dei suesposti diritti, il Regolamento afferma che è opportuno prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diversi diritti previsti (considerando 59). Queste "modalità" agevolative possono consistere ad esempio in mezzi organizzativi o anche tecnologici, come appositi form sul sito, apposite sezioni sulle App o perfino mezzi di interazione diretta con i dati stessi. In particolare, il Regolamento richiede che qualora i dati personali siano trattati con mezzi elettronici, il titolare dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica.

Una volta che l'interessato richiede l'esercizio dei diritti, poi, la regola generale è che il titolare del trattamento risponda alle richieste dell'interessato «*senza ingiustificato ritardo e al più tardi entro un mese*» e motivi la sua eventuale intenzione di non accogliere tali richieste (considerando 59). A differenza della previgente Direttiva, dunque, si pone una regola generale riguardo ai tempi di reazione alle richieste degli interessati: in assenza di una diversa specifica previsione di tempo, l'esercizio dei diritti dovrebbe essere garantito in non oltre 30 giorni. Peraltro, qualsiasi diniego alle richieste degli utenti va specificamente motivato.

*

VI.- I soggetti: profili generali

Da ultimo, è opportuno passare in rassegna le figure coinvolte nel trattamento dati secondo quanto indicato dal GDPR.

Titolare: Persona, fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità e modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza

Responsabile: Persona, fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo, preposti dal Titolare al trattamento

Incaricato: Persona fisica autorizzata a compiere operazioni di Trattamento sulla base delle istruzioni ricevute dal Titolare e/o dal Responsabile

Interessato: Persona fisica titolare dei dati

Data Protection Officer: è obbligatoria solo in alcuni casi:

- Se il titolare è un soggetto pubblico;
- Se l'attività principale del Titolare consiste in trattamenti che, per loro natura, ambito di applicazione o finalità comportano il monitoraggio regolare e sistematico degli interessati "su larga scala",
- se l'attività principale del Titolare consiste in trattamenti regolari e sistematici di dati particolari o giudiziari

La nomina del DPO non dipende dal numero di soci, ma dalla tipologia di trattamento effettuata e dal rischio cui si espongono i dati.

Può essere un soggetto esterno o interno all'azienda, deve avere requisiti di professionalità e di esperienza commisurati alla sensibilità, complessità e quantità di dati trattati e deve godere di indipendenza ed autonomia di spesa.

Ha compiti specifici:

- Informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento;
- Predisporre relazioni periodiche per il management;
- Sorvegliare l'osservanza del Regolamento e di tutte le altre disposizioni anche nazionali in materia di protezione dei dati;
- Vigilare che il Titolare ed il Responsabile conferiscano nomine a soggetti adeguati;
- Verificare l'adozione di policy adeguate;
- Sensibilizzare e formare il personale che partecipa ai trattamenti e alle attività di controllo;
- Assistere il Titolare nello svolgimento della valutazione di impatto;
- Predisporre e mantenere aggiornato il registro dei trattamenti;
- Cooperare con l'Autorità di controllo.

* * *

Parte Speciale

Di seguito, si procede con l'indicazione di una serie di consigli pratici utili per l'adeguamento alla normativa contenuta nel GDPR

*

L'ampliamento della definizione di dato personale

L'art. 4, par. 1, n. 1 del GDPR definisce il Dato personale come «*qualsiasi informazione riguardante una persona fisica identificata o identificabile*». Per stabilire l'identificabilità di un interessato, il GDPR suggerisce di considerare tutti i mezzi di cui il Titolare o un terzo può ragionevolmente avvalersi per identificare detto Interessato, direttamente o indirettamente.

Conseguenze pratiche: *in caso di dubbi sull'interpretazione o identificazione di un'informazione come Dato personale, si suggerisce di trattare quell'informazione come se fosse un Dato personale, nella sua più ampia accezione.*

In considerazione del fatto che il GDPR ha introdotto un sistema di compliance privacy più rigido, connotato da sanzioni pecuniarie particolarmente elevate, si suggerisce, al fine di minimizzare i rischi, di non trattare, quando è possibile, Dati personali, oppure nel caso in cui vadano trattati di adottare tutte le più opportune misure tecniche e organizzative per conformarsi al GDPR.

Se c'è un elevato grado di identificabilità dell'Interessato e i suoi Dati personali vanno trattati, si suggerisce di usare la tecnica della pseudonimizzazione.

*

Il principio dell'accountability

I titolari devono assicurarsi che i Trattamenti da loro effettuati siano conformi ai principi *privacy* previsti all'art. 5, par. 1, del Regolamento, tra i quali particolare rilievo assumono quelli della trasparenza e delle minimizzazione dei dati.

Conseguenze pratiche: *i Titolari devono rivedere o aggiornare gli esistenti programmi di compliance privacy.*

I Titolari devono sviluppare o, laddove già esistenti, aggiornare le policy interne e i piani di risposta dei Data Breach.

È opportuno destinare parte delle risorse economiche accantonate per la compliance privacy alla formazione dei dipendenti. I programmi di formazione dovranno essere strutturati in modo da offrire una conoscenza generale e complessiva del Gdpr, ma soprattutto dovranno adattare e calare la privacy nel settore in cui opera il titolare

*

L'osservanza delle condizioni di liceità

I Titolari sono tenuti a riesaminare tutti i Trattamenti attuali e ad assicurarsi che per ogni Trattamento, anche futuro, esista una base giuridica che lo giustifica e, in caso di assenza, appurare quale sia l'esenzione o la deroga.

Conseguenze pratiche: *si consiglia di documentare sempre quale sia la base giuridica del trattamento e di illustrare brevemente le ragioni di tale scelta.*

Quando la base giuridica del Trattamento è il consenso dell'Interessato, i Titolari sono tenuti a dimostrare di averlo acquisito in conformità al GDPR o, in caso contrario, a revisionare gli attuali meccanismi preposti alla raccolta del consenso. Se, invece, detta base è un intervento legittimo, i Titolari sono tenuti a documentare e a mantenere traccia di simile base giuridica nel Registro.

*

L'informativa privacy

È diritto dell'interessato di essere compiutamente informato sui Trattamenti che hanno ad oggetto i Suoi Dati personali.

Conseguenze pratiche: *i titolari sono tenuti a:*

- *pianificare il linguaggio da usare nelle informative: si devono evitare espressioni gergali, troppo tecniche o giuridiche;*
- *predisporre informative concise, intellegibili e facilmente accessibili, scritte con linguaggio semplice e chiaro. Informative eccessivamente lunghe o troppo complesse non saranno ritenute conformi al Gdpr.*

Si suggerisce ai Titolari di fornire una breve sintesi dei punti chiave del trattamento e delle Finalità perseguite, e di mettere a disposizione dell'interessato un link dove potrà trovare la policy privacy contenente un maggior dettaglio su come vengono usati i Dati oggetto di Trattamento.

I Titolari possono usare informative aggiuntive nel caso in cui il titolare si interfacci con Interessati appartenenti a categorie particolari (ad esempio, minori).

I Titolari possono informare gli Interessati anche con strumenti alternativi al cartaceo (ad esempio, video).

*

Il Consenso

Come detto, il consenso rimane la principale base giuridica per il Trattamento. Tuttavia, con il Gdpr, diventa più difficile, per il Titolare, ottenere un consenso valido.

Conseguenze pratiche: *il consenso deve essere specifico, cioè riferito ad un particolare Trattamento espressamente illustrato, e informato, dovendo l'Interessato ricevere dal Titolare tutte le informazioni necessarie per capire in cosa consiste il Trattamento e per quali finalità è effettuato.*

Il consenso è il risultato di un comportamento attivo o di una dichiarazione positiva dell'Interessato, che ha chiaramente manifestato l'intenzione di far trattare i suoi Dati personali dal Titolare.

In definitiva:

1. i Titolari devono assicurarsi che gli Interessati siano debitamente informati, prima di rilasciare il Consenso, su cosa consiste il trattamento;

2. Sebbene siano liberi di adottare il meccanismo o il metodo di raccolta del Consenso più appropriato, i Titolari del Trattamento sono tenuti ad adottare meccanismi di raccolta del consenso che siano ben parametrati sulla natura del consenso richiesto.

3. I meccanismi di raccolta del consenso devono essere ideati in modo da garantire il rilascio di un consenso facoltativo e genuino da parte dell'interessato. Non possono essere previsti meccanismi di silenzio-assenso, acquiescenza passiva o box preselezionati su internet del Titolare.

4. I Titolari sono obbligati a prevedere dei meccanismi che assicurino agli Interessati la revoca immediata del Consenso.

*

Policy privacy

Al fine di consentire all'interessato l'esercizio delle nuove tutele e dei diritti previsti dal GDPR, è opportuno che il Titolare riveda le proprie procedure interne e formi i dipendenti che si interfacciano con i Clienti, persone fisiche, in modo tale da predisporre dei processi che siano conformi all'art. 15 del Gdpr.

Conseguenze pratiche:

- il Titolare potrebbe prendere in considerazione l'ipotesi di creare portali sui propri siti internet dove consentire all'interessato di esercitare direttamente il diritto di accesso;

- il Titolare deve accertarsi che i membri del suo staff e il suo personale abbiano riconosciuto e sappiano come gestire un'istanza di limitazione al Trattamento. Si deve procedere ad una verifica dei sistemi interni e delle procedure implementate per appurare se essi siano conformi ai requisiti del GDPR e, cioè, se siano strutturati in modo tale da agevolare la richiesta dell'Interessato;

- Vanno revisionate e aggiornate le informative e le privacy policy in modo tale da assicurare all'interessato una piena conoscenza della possibilità di esercitare il diritto all'opposizione. Tale informativa va fornita, in modo chiaro e separato, dal Titolare al primo contatto con l'Interessato.

Per i Titolari che erogano servizi online, bisogna prevedere degli strumenti che consentano l'esercizio del diritto di opposizione e l'accoglimento della richiesta in modo automatico;

*

DPIA

Il DPIA può essere qualificato come un processo aziendale complesso finalizzato a descrivere il trattamento, valutarne il rispetto dei principi di necessità e proporzionalità, identificare i rischi per i diritti e le libertà delle persone fisiche derivante da tale Trattamento e le conseguenti misure di sicurezza da implementare a protezione dei Dati Personali che si intendono trattare.

Il DPIA contiene:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Quando effettuare il DPIA:

- Trattamenti valutativi o di *scoring* dell'interessato, compresa la profilazione e attività predittive:
  - Istituto finanziario che effettua screening dei propri clienti;
  - Società che offre test genetici per finalità predittive del rischio di determinate patologie.

- Decisioni automatizzate che producono significativi effetti giuridici:
  - Il Trattamento può comportare l'esclusione di un Interessato da determinati benefici ovvero la sua discriminazione.

- Monitoraggio sistematico:
  - Trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la sorveglianza sistematica di un'area aperta al pubblico.

- Trattamenti dati sensibili o di natura strettamente personale
  - Un ospedale che conserva le cartelle cliniche dei pazienti;
  - Un'azienda farmaceutica che conserva le ricette.

- Trattamento di dati su larga scala:
  - Quando un trattamento riguarda un numero di interessati elevati rispetto alla popolazione di riferimento; elevato volume di dati personali trattati; durata o persistenza del Trattamento; ambito geografico del trattamento.

- Trattamento di Dati personali relativi a interessi vulnerabili:
  - Minori;
  - Soggetti con patologie psichiatriche;
  - Richiedenti asilo;
  - Pazienti.

- Trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un contratto:
  - Screening dei clienti di una banca attraverso i Dati registrati in una centrale rischi al fine di stabilire se ammetterli ad un finanziamento.

- Combinazioni o raffronto di dati di insiemi di Dati personali.

*

Titolare, contitolare e responsabile

Il Titolare è la persona fisica o giuridica che stabilisce le Finalità del Trattamento e le modalità operative del suo espletamento.

Quando, con riferimento ad un singolo Trattamento, due o più entità decidono e determinano congiuntamente le Finalità e i mezzi del Trattamento, queste sono contitolari del Trattamento.

In molte circostanze, un Trattamento viene ad articolarsi in una serie di operazioni e/o attività svolte ciascuna delle quali da due o più Titolari differenti, ma tra loro collegati.

Il GDPR obbliga i contitolari a sottoscrivere un accordo interno con cui vengono ripartite le responsabilità e stabiliti i ruoli dei soggetti.

Il contenuto dell'accordo deve essere sintetizzato e messo a disposizione degli Interessati.

Il GDPR rende i contitolari pienamente responsabili nei confronti dell'Interessato.

Il Responsabile è colui che tratta i dati per conto del Titolare.

Il titolare, dunque, oltre al DPO, ove necessario, deve altresì indicare il responsabile del trattamento.

* * *