IL REGOLAMENTO GENERALE EUROPEO N. 679/2016 (GDPR)

REGOLE E ADEMPIMENTI PRATICI PER L'AMMINISTRATORE DI CONDOMINIO

LE FONTI

- GDPR: il Regolamento Generale Europeo n. 679/2016
- Codice Privacy (D.Lgs. 196/03 e D.Lgs. 101/18)
- Regole Deontologiche e Codici di condotta
- Linee guida WP29
- Linee guida dell'Autorità Garante italiana

I PRINCIPI

- Dati personali e trattamento di dati personali
- I Ruoli nel trattamento (titolare e contitolare, responsabile, autorizzati, responsabile della protezione dei dati)
- L'Art. 5 del GDPR: i principi applicabili al trattamento
- L'Art. 6 del GDPR: Liceità del trattamento
- L'Accountability: l'Art. 24
- L'Art. 25: *Privacy by design* e *by default*
- Introduzione ai diritti (cenni)
- La Valutazione di impatto sulla protezione dei dati (cenni)
- Data Breach (cenni)

ADEMPIMENTI PRATICI

- Lo Studio Professionale e gli Enti Amministrati
- Come procedere. Gli adempimenti adeguati
- L'aggiornamento e il mantenimento della *compliance*

1. LE FONTI

1.1. IL GDPR: REGOLAMENTO EUROPEO N. 679/2016[1]

Il **Regolamento Generale Europeo del 27 aprile 2016, n. 679**, relativo alla protezione dei delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, entrato in vigore nel maggio del 2016, ha trovato piena applicazione in tutti gli Stati membri dell'Unione a partire dal 25 maggio 2018[2].

Il c.d. "G.D.P.R." introduce un regime normativo sostanzialmente identico, in materia di protezione dei dati personali, in tutto il territorio europeo, così limitando le asimmetrie prodotte dai diversi interventi degli Stati membri nell'applicazione della precedente "Direttiva Madre", la **Direttiva 95/46/CE**[3], oltre che dalle diverse concrete applicazioni talvolta operate dalle singole Autorità di Controllo, ossia dai Garanti nazionali[4].

L'idea comune europea di dare uniformità alle norme in materia di protezione e trattamento dei dati personali e alla loro applicazione è confermata dalla istituzione della nuova Autorità di controllo europea, l'*European Data Protection Board* (***EDPB***: v. *infra*), con il potere di indirizzo mediante l'adozione di provvedimenti, indicazioni e Linee Guida, così come di risolvere eventuali contrasti tra le singole Autorità nazionali.

La necessità di una **nuova e più moderna, oltre che uniforme, regolamentazione della "privacy"** era ed è sotto gli occhi di tutti[5]: nell'ultimo decennio le imprese il cui *core business* è basato sul commercio elettronico o, comunque, sul *trading* dei dati personali è aumentato esponenzialmente, sia facendo emergere nuove modalità di raccolta, gestione e utilizzo dei dati personali, sia modificando vecchi e tradizionali settori, che si sono adeguati al cambiamento. Non sono mancati, negli ultimi anni, scandali, furti, perdite di dati e utilizzo manipolatorio degli stessi[6].

La protezione delle persone fisiche con riguardo al trattamento dei dati personali era già stata individuata dalla Carta dei diritti fondamentali

---

[1] *Contributo informativo a carattere editoriale, da non intendersi sostitutivo di un parere o di una consulenza legale, elaborato per Anaci Veneto nel mese di marzo 2020, a supporto del materiale audio e video edito.*

[2] https://www.garanteprivacy.it/il-testo-del-regolamento.

[3] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/432175.

[4] "Privacy is not dead: it's hiring", R. PANETTA, in *Commentario al Reg. UE n. 2016/679 e al novellato d.lgs. 196/2003*, Giuffrè Francis Lefebvre, 2019, cap. I, pagg. 3 e ss..

[5] Si vedano le dichiarazioni del Garante Antonello Soro, nel luglio 2019: *"Il livello di consapevolezza è cresciuto, anche grazie a vicende come il Datagate di Snowden o Cambridge Analytica, ma è ancora primitivo. Bisogna far capire anche alla politica che il dato da una parte rappresenta un valore economico straordinario; ma dall'altra è un oggetto di diritto fondamentale, la proiezione della nostra persona nella dimensione digitale. Si tende a considerare la privacy come residuale, anteponendole altre esigenze come la sicurezza, il controllo: telecamere, impronte, dati biometrici dei lavoratori. In gioco c'è il diritto alla libertà, che non si può monetizzare. Proteggere i dati significa libertà di non essere assoggettati a un'opera di profilazione prima e poi di indirizzamento occulto nelle scelte che facciamo"*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9115279.

[6] Tra le molte pubblicazioni sul tema del trattamento dei dati personali, degli algoritmi e del mercato e sulle problematiche che ne discendono si veda, da ultimo: M. DELMASTRO – A. NICITA, Big Data. Come stanno cambiando il nostro mondo, Il Mulino, Bologna, 2019.

dell'unione Europea come un diritto fondamentale di ogni individuo (Carta di Nizza, art. 8, par. 1[7]). Il Regolamento intende "contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche."[8]

"La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata", negli ultimi anni, in modo estremamente significativo e non pare avere limiti. Le attuali tecnologie "consentono tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali come mai in precedenza .... Sempre più spesso le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano."[9]

Un'evoluzione di tal genere "**richiede un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di attuazione**", al fine di "creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche."[10]

Si inserisce nel quadro appena delineato da alcuni "Considerando", il c.d. GDPR, che introduce un nuovo complesso di norme applicabili a tutti gli Stati membri e modifica in modo sostanziale diverse leggi nazionali, come ad esempio il nostro Codice Privacy, il d.lgs. 196/2003.

1.2. IL CODICE PRIVACY IL D.LGS. 196/2003, MOD. DAL D.LGS. 101/2018

Successivamente al Regolamento Europeo n. 679/2016 in Italia è stato emanato un decreto di adeguamento della normativa nazionale in tema di protezione dei dati personali: il **D.Lgs. 101/2018**[11], entrato in vigore il 19 settembre 2018, che ha provveduto:

a) ad abrogare le norme del Codice Privacy (d. lgs. 196/2003) incompatibili con la nuova normativa europea, a

b) introdurne delle nuove e a modificane e integrarne altre, il tutto al fine di **armonizzare e specificare la normativa italiana**.

Sintetizzando, si può dire che gli **aspetti positivi** del provvedimento riguardano:

[7] http://www.giurcost.org/fonti/CdfUE.pdf.
[8] V. il Considerando 2 del Regolamento n. 679/2016. I Considerando (*Whereas*) costituiscono le "premesse" all'articolato del Regolamento, composto da ben 173 di tali essi e da 99 articoli: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[9] Considerando n. 6.
[10] Considerando n. 7.
[11] https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.

- Una maggiore chiarezza del quadro normativo nazionale.
- L'abrogazione delle Misure minime di sicurezza (il c.d. All. "B" Cod. Privacy; per alcuni dettagli, si veda *infra*).
- La semplificazione della disciplina dei trattamenti dati in ambito sanitario e la previsione dell'adozione, da parte dell'Autorità Garante, delle Misure di Garanzia (art. 2 - *septies* del Codice Privacy).
- L'attualizzazione delle Autorizzazioni Generali mediante appositi provvedimenti del Garante a seguito di consultazione pubblica.
- Il mantenimento dei Codici di deontologia o buona condotta, trasformati nelle Regole Deontologiche.
- La previsione della possibile rappresentanza degli interessati dinanzi al Garante tramite le Associazioni di categoria.
- L'introduzione di possibili meccanismi di semplificazione per Micro, Piccole e Medie imprese.
- La previsione di fattispecie penali a tutela di interessi primari.
- L'espressa previsione della validità del consenso minori in relazione ai servizi della società dell'informazione a partire dai 14 anni[12].
- La previsione di alcuni diritti riguardanti le persone decedute, assicurando ai superstiti strumenti efficaci di accesso e controllo del patrimonio informativo del defunto o relativo allo stesso, diversamente relegato in una sfera di difficile gestibilità[13].
- Per quanto riguarda i rapporti di lavoro, il d.lgs. 101/2018, all'art. 111, intervenendo, come previsto dalla normativa europea, ha stabilito che il Garante promuove l'adozione di Regole Deontologiche anche in tali ambiti, ai sensi dell'art. 2 – *quater* del medesimo Codice[14].
- Vale la pena ricordare come l'art. 111 – *bis*, del Codice, rubricato "Informazioni da fornire in caso di ricezione di *curriculum*", stabilisca che le informazioni da fornire all'interessato ai sensi dell'art. 13 del GDPR, ossia la c.d., nella terminologia precedente, "Informativa", debbano essere rese, in caso di ricezione dei *curricula* spontaneamente inviati, in occasione del primo contatto successivo all'invio del *curriculum* stesso.
- La previsione di appositi soggetti "designati" cui il titolare può attribuire specifici compiti e funzioni connesse al trattamento dei dati personali nell'ambito della propria organizzazione[15].

---

[12] L'art. 8 del GDPR, infatti, prevede che, nell'ipotesi in cui la base giuridica legittimante il trattamento dei dati personali sia il consenso dell'interessato (art. 6, par. 1, lett a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento dei dati personali degli stessi sia lecito ove il minore abbia almeno 16 anni di età. Il decreto di adeguamento ha stabilito, con l'introduzione del nuovo art. 2 – *quinques*, una età differente, fissandola, a 14 anni. Deve essere evidenziato come tale limite d'età si riferisca esclusivamente al consenso rilasciato per il trattamento dei dati nell'ambito della *fornitura di un servizio della società dell'informazione* che, in base alla Direttiva 98/34/CE come modificata dalla Direttiva 98/48/CE, si riferisce a qualsiasi servizio, normalmente prestato dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1998L0034:19980810:IT:PDF.

[13] In particolare, a soggetti portatori di un interesse proprio in relazione alle informazioni del deceduto, a terzi che si trovino in una relazione qualificata con lo stesso per ragioni familiari meritevoli di protezione e agli stessi interessati che lascino disposizioni sul trattamento dei propri dati a seguito del decesso, viene riconosciuta la possibilità, sostanzialmente, di un controllo delle citate informazioni: si veda art. 2 – *terdecies* del C. Privacy.

[14] Si veda, quale riferimento, l'art. 88 del GDPR: "gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali nell'ambito del rapporto di lavoro".

[15] Art. 29 – *quaterdecies*. Sia consentito rinviare a quanto brevemente indicato in https://www.eclegal.it/soggetti-trattano-dati-personali/.

- La previsione che chiunque possa provvedere a inviare una segnalazione al Garante (art. 144 Cod. Privacy).
- La duplice previsione del Reclamo al Garante (art. 77 GDPR e artt. 140 – *bis* – 143 Cod. Privacy) o del Ricorso all'Autorità Giudiziaria.
- Ai fini della presente esposizione si ricordano poi le violazioni amministrative, le cui ipotesi e procedura sono previste dall'art. 166 e gli illeciti penali, per i quali si rinvia agli artt. da 167 a 172.

Non mancano, ovviamente, alcuni aspetti, per così dire, "**in ombra**" della riforma del Codice come, per esempio, il fatto che il d.lgs. 101/208, quanto alla forma, provveda con due serie di articoli, con gli uni di emenda del Codice, con gli altri, invece, di indifferenziata applicazione, con il che le fonti normative da tenere presente sono costituite non solo dal Regolamento Europeo e del Codice novellato, ma anche da diversi articoli dello stesso Decreto 101/2018.

Per altri versi si è optato per numerosi articoli con sotto specificazioni (Art. 2 *bis* … Art. 2 *septiesdecies*). Da altro punto di vista il testo appare pesantemente normativo[16].

1.3. I CODICI DI CONDOTTA

Al fine di contribuire alla corretta applicazione del Regolamento gli Stati membri, le Autorità di Controllo e la Commissione incoraggiano l'elaborazione dei Codici di condotta di cui all'art. 40 del GPDR. Detti Codici, in particolare, dovrebbero essere adottati da associazioni o altre organizzazioni che rappresentano le categorie di titolari o responsabili al fine di procedere a una regolamentazione che risponda alle esigenze di micro, piccole e medie imprese raggruppabili in "settori di trattamento". L'obiettivo, in particolare, è non solo quello di **garantire una applicazione coerente e omogenea del Regolamento**, ma anche di **bilanciare gli interessi di particolari categorie di titolari** nei confronti dei relativi interessati, per evitare sbilanciamenti[17].

Per tali motivi anche le associazioni e gli altri organismi rappresentanti le categorie di titolari o responsabili possono elaborare codici di condotta, modificarli o prorogarli allo scopo di precisare l'applicazione del regolamento, ad esempio relativamente a:

a) Trattamento corretto e trasparente,
b) Legittimi interessi perseguiti in settori specifici,
c) Raccolta dei dati,
d) Pseudonimizzazione,
e) L'informazione fornita al pubblico e agli interessati,
f) L'esercizio dei diritti,
g) L'informazione fornita al minore e le modalità di ottenimento del relativo consenso,

[16] L.BOLOGNINI e E.PELINO, *Codice Privacy, tutte le novità del d.lgs. 101/2018*, Il Civilista, Giuffrè Francis Lefebvre, 2018, pag. 11.
[17] L. BOLOGNINI, *Commentario al Reg. UE n. 2016/679 e al novellato d.lgs. 196/2003*, Giuffrè Francis Lefebvre, 2019, pag. 286.

h) Le misure e le procedure di cui agli artt. 24 e 25 del Regolamento (v. *infra*),
i) Le notifiche e le comunicazioni in caso di incidenti di violazione,
j) Il trasferimento verso paesi terzi,
k) Le procedure per comporre le controversie tra titolari o interessati.

I Codici, si tratti di approvazione, modifica o proroga, sono approvati dall'Autorità con una procedura standardizzata che prevede un parere, distinguendosi, ulteriormente, le ipotesi in caso di codici aventi validità generale o in codici cui possano aderire titolari non soggetti al Regolamento Europeo[18].

L'importanza dei Codici di condotta può essere evidenziata sotto un duplice aspetto. Il primo è dato dalla previsione del paragrafo 3 dell'art. 24, in base al quale **l'adesione agli stessi[19] può essere utilizzata come elemento per dimostrare il rispetto degli obblighi** del titolare del trattamento mentre, come vedremo tra poco, le Regole Deontologiche contengono norme e disposizioni la cui osservanza costituisce condizione essenziale di liceità del trattamento dei dati personali[20]. Il secondo è dato dal rilievo che, operando nel senso dell'agevolazione dell'opera di titolari e responsabili in diversi settori e ambiti di applicabilità del Regolamento stesso[21], i Codici possono **orientare operativamente e concretamente l'attività dei titolari**.

1.4. LE REGOLE DEONTOLOGICHE

In base all'art. 2 *quater* del Codice Privacy modificato dal d.lgs. 101/2018 il Garante promuove l'adozione (e verifica la conformità alle disposizioni vigenti) di tali Regole per i trattamenti previsti per adempiere un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per i trattamenti di dati genetici, biometrici o relativi alla salute, per i trattamenti relativi a libertà di informazione e d'espressione, di accesso del pubblico a documenti ufficiali, trattamenti di dati nell'ambito del rapporto di lavoro, garanzie o deroghe nell'ambito di trattamenti ai fini di archiviazione nel pubblico interesse, di ricerca scientifica e storica o a fini statistici, obblighi di segretezza professionale, ecc..

La procedura prevede, sostanzialmente, la consultazione dei soggetti e degli enti "portatori di interesse" e la discussione su un primo testo di proposta, definito il quale lo schema viene sottoposto a consultazione pubblica per almeno sessanta giorni. Decorsa la fase della consultazione, le Regole, approvate dal Garante, vengono pubblicate sulla Gazzetta Ufficiale e riportate nell'Allegato A del Codice.

[18] Si vedano, per il dettaglio, i paragrafi 6. e 7. Del Regolamento.
[19] O a un meccanismo di certificazione ex art. 42.
[20] L.BOLOGNINI e E.PELINO, *Codice Privacy, tutte le novità del d.lgs. 101/2018*, Il Civilista, Giuffrè Francis Lefebvre, 2018, pag. 51.
[21] Si vedano, a titolo esemplificativo: l'art. 28.5 sulle garanzie sufficienti nella designazione del Responsabile del trattamento, laddove l'adesione da parte di questi a un Codice approvato (o a un meccanismo di certificazione) costituisce un "elemento per dimostrare la conformità"; l'art. 32.3, sulle misure di sicurezza; l'art. 35.8, sulla valutazione di impatto, e così via.

Quel che mette conto evidenziare (e qui sta anche la differenza, già segnalata, rispetto ai Codici di condotta: *supra*) è che in base all'art. 2, quater, n. 4., "**il rispetto delle** disposizioni contenute nelle **Regole costituisce condizione essenziale per la liceità e la correttezza dei trattamenti" effettuati**[22].

1.5. LE LINEE GUIDA WP 29 (OGGI EDPB)

Le Linee Guida **mirano a fornire indicazioni di carattere generale** in relazione al trattamento di dati personali in vari ambiti, **al fine di garantire la corretta applicazione dei principi** stabiliti dalle norme.

Il Gruppo di lavoro "Articolo 29" (Art. 29 WP) è il gruppo di lavoro europeo indipendente che ha trattato questioni relative alla protezione della vita privata e dei dati personali fino al 25 maggio 2018 (entrata in vigore del GDPR). L'*European Data Protection Board*, o Comitato europeo per la protezione dei dati (**EDPB**) è l'organismo che ha sostituito il Gruppo di lavoro articolo 29 (appunto perché previsto dall'art. 29 della direttiva europea 95/46/CE), col nuovo regolamento europeo, ed è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.

E' un organismo consultivo indipendente, composto da un rappresentante della varie autorità nazionali, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta.

L'articolo 70 del GDPR affida al Comitato dei Garanti nazionali diversi compiti, allo scopo:

- di assicurare la corretta applicazione del regolamento;
- fornire consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione;
- **pubblicare linee guida, raccomandazioni e prassi al fine di promuovere l'applicazione coerente del regolamento** e sulle materie previste;
- esaminare, di propria iniziativa o su richiesta di uno dei membri o della Commissione, qualsiasi questione relativa all'applicazione del regolamento;
- effettua l'accreditamento di organismi di certificazione e il suo riesame periodico;
- fornire alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale;
- promuovere la cooperazione e l'effettivo scambio di informazioni e prassi tra le autorità di controllo a livello bilaterale e multilaterale;
- promuovere programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di organizzazioni internazionali;

[22] Ad oggi sono state approvate e pubblicate le seguenti Regole:
A.1. Trattamento dati nell'esercizio dell'attività giornalistica,
A.2. Trattamento dati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria,
A.3. Trattamento a fini di archiviazione nel pubblico interesse o per scoi di ricerca storica,
A.4. Trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del S.S.N.,
A.5. Trattamenti a fini statistici o di ricerca scientifica.

- emettere pareri sui codici di condotta;
- tenere un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza.

Il compito principale è dunque garantire il principio di congruità e coerenza, ossia assicurare che le autorità di controllo nazionali seguano interpretazioni comuni della normativa europea in materia.

1.6. LE LINEE GUIDA DEL GARANTE PRIVACY

Si inseriscono in questo quadro anche le Linee Guida del Garante nazionale, le quali sono intese a fornire indicazioni di carattere generale in relazione al trattamento di dati personali in vari ambiti, al fine di **garantire la corretta applicazione dei principi** stabiliti dal Regolamento Europeo, dal Codice Privacy e dalla normativa applicabile[23].

2. I DATI PERSONALI

2.1. Dati personali

Ai sensi dell'**art. 4**[24], **par. 1, n. 1)**, è

> "*dato personale **qualsiasi informazione riguardante una persona fisica identificata o identificabile** ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on-line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.*"

I dati personali riguardano quindi le informazioni sugli individui, sulla loro vita privata come su quella pubblica o le relative attività professionali.

Se una informazione si riferisce ad una persona identificata o identificabile, essa è un dato personale[25]. La possibile identificabilità di un soggetto necessita di valutazioni costanti, giacché un'informazione contiene dati personali riguardanti una persona fisica se questa è identificata o identificabile in base a tali informazioni, ma anche se possa essere individuata mediante l'utilizzo di tali informazioni in modo da consentire di svelarne l'identità con l'utilizzo di altre ricerche. Non ha rilevanza, in tale contesto, di quale tipologia o forma di

[23] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1772725.
[24] L'art. 4 del Regolamento è rubricato "Definizioni".
[25] Si veda il Manuale Europeo sulla Protezione dei Dati Personali, pag. 97: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_it.pdf.

informazioni si disponga (documenti elettronici o cartacei, archivi, campioni, immagini, suoni, ecc.): il rilievo preminente rimane **la possibile identificabilità**.

Il Considerando 26 del Regolamento chiarisce che il parametro di riferimento è dato dalla valutazione della disponibilità, in capo a potenziali utenti di tali informazioni, ma anche di utenti terzi, di ragionevoli mezzi identificativi: con il che una persona non è considerata identificabile se tale identificazione richiede sforzi, costi e tempi irragionevoli.

2.2. Categorie particolari di dati personali

In tale categoria di dati personali (**art. 9**) rientrano gli "ex" dati sensibili del Codice Privacy e i dati biometrici e genetici, unitamente ai dati idonei a rivelare opinioni politiche, origini razziali, appartenenza a gruppi politici o sindacali, l'orientamento e le abitudini sessuali.

Dati genetici: sono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona e che forniscono indicazioni univoche sulla fisiologia o sulla salute, come avviene per i campioni biologici.

I dati biometrici sono dati ottenuti mediante uno specifico trattamento relativo alle caratteristiche fisiche, fisiologiche o comportamentali di un individuo, atte a confermare o meno la relativa identificazione univoca, come l'immagine del viso o le impronte dattiloscopiche.

I **dati relativi alla salute** sono, in generale, i dati attinenti la salute fisica o mentale di un individuo, comprese le prestazioni di servizi di assistenza sanitaria, che rivelano o forniscono indicazioni e informazioni relative alla salute.

I **dati giudiziari** sono previsti dall'**art. 10**[26].

3. I TRATTAMENTI – TIPOLOGIE

La definizione di trattamento dei dati personali è contenuta nell'**art. 4, p. 1, n. 2)**:

> "***qualsiasi operazione o insieme di operazioni***, *compiute con o senza l'ausilio di processi automatizzati e* ***applicate a dati personali*** *o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a*

[26] Art. 10: Trattamento dei dati personali relativi condanne penali e reati.

disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione."

Come si vede, il concetto di trattamento è molto ampio, giacché si applica a tutti i trattamenti **automatizzati ma anche** ai trattamenti **non automatizzati laddove i dati personali siano contenuti in un archivio** o destinati a figurarvi.

Quest'ultimo (archivio) è un qualsiasi insieme di dati personali, strutturato, accessibile secondo criteri determinati, indipendentemente dal fatto che detto archivio sia o meno centralizzato o ripartito in modo funzionale o geografico.

Vale la pena evidenziare come sia considerata trattamento un'attività di qualsiasi genere svolta con o in relazione a dati personali, anche se di tipo non trasformativo: il Garante italiano, ad esempio, considera attività di trattamento anche un mero possibile accesso, come avviene nel caso di videosorveglianza senza registrazione. Non rileva neppure che l'attività sia diretta a conoscere il contenuto informativo del dato: si tratta anche in tal caso di trattamento[27].

4. I RUOLI NEL TRATTAMENTO DI DATI PERSONALI

4.1. TITOLARE DEL TRATTAMENTO E CONTITOLARI

Il **Titolare** del trattamento dei dati personali è definito, nell'**art. 4, p. 1, n. 7)**, come

"*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**;*

quando le finalità e i mezzi ... sono determinati dal diritto dell'Unione Europea o degli altri Stati membri, il titolare del trattamento o i criteri applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione Europea o degli Stati membri...".

L'art. 24 del GDPR pone precise responsabilità in capo a colui che, esercitando le proprie prerogative, ha il potere di determinare e scegliere come agire; da ciò deriva che egli ne sopporterà, anche, le conseguenze (è il c.d. principio della responsabilizzazione[28]).

[27] Si veda il commento all'art. 4 in Codice di disciplina della Privacy, diretto da L. Bolognini e E. Pelino, Giuffrè Francis Lefebvre, 2019.
[28] Soggetti del trattamento dei dati personali - PRIVACY. Protezione e trattamento dei dati. IPSOA MANUALI – WOLTERS KLUWER, 2020, pag. 156.

Dirimente risulta dunque il potere direttivo sui due elementi delle **a) finalità** e dei **b) mezzi** del trattamento, anche al fine di distinguere la figura del titolare da quella del Responsabile (v. *infra:* 4.2.).

Le finalità possono essere definite come gli scopi o gli obiettivi per i quali il titolare svolge le operazioni di trattamento: il datore di lavoro, ad esempio, tratta i dati personali dei propri dipendenti ai fini di dare corso al rapporto lavorativo; un'impresa tratta i dati personali (oltre che dei propri dipendenti ai fini di gestione del rapporto di lavoro) anche dei propri fornitori e dei propri clienti o possibili clienti ai fini della gestione amministrativa, contabile, contrattuale del complessivo rapporto.

La possibilità e il potere di determinare le finalità del trattamento costituiscono gli indici che consentono l'individuazione del titolare e, nel contempo, l'individuazione e la specificazione del limite ai dati personali da trattare, dell'ambito della circolazione degli stessi, della durata della conservazione[29].

E', dunque, il titolare del trattamento dei dati personali il soggetto, l'ente o l'organismo che ha il potere di pianificare e attuare le scelte strategiche e organizzative in merito alle modalità e ai criteri di raccolta, conservazione, utilizzo, elaborazione dei dati personali e, insieme, di determinazione delle misure tecniche e organizzative di sicurezza da adottare[30].

Allorché due o più titolari determinino **congiuntamente** le finalità e i mezzi del trattamento, essi sono considerati **Contitolari**: decidono insieme di trattare i dati per una finalità comune.

In tali casi, sostanzialmente, il potere decisionale è condiviso con altri, anche in modo non simmetrico[31].

4.2. RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento è definito nel Regolamento come

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

Tale soggetto, dunque, non determina finalità e mezzi del trattamento (*purposes and means*), fatte salve le scelte in materia di sicurezza e i relativi

[29] Si veda il commento all'art. 4 in Codice di disciplina della Privacy, diretto da L. Bolognini e E. Pelino, Giuffrè Francis Lefebvre, 2019, pag. 45.
[30] *Commentario al Reg. UE n. 2016/679 e al novellato d.lgs. 196/2003*, Giuffrè Francis Lefebvre, 2019, pag. 149.
[31] Si veda il parere n. 1/2010 del Gruppo di Lavoro WP29: https://www.garanteprivacy.it/documents/10160/10704/wp169+-+Parere+1+2010+sui+concetti+di+responsabmile+del+trattamento+e+incari.pdf/64cd4700-f0d4-4c04-b834-9c3da69a93ea?version=1.1, a tutt'oggi ancora il parere più completo ed esaustivo sui concetti di Titolare, Contitolare e Responsabile del trattamento.

profili tecnici e organizzativi bensì, su delega del titolare, effettua operazioni di trattamento su dati personali che non ha direttamente raccolto.

Le attività affidate a un responsabile possono essere limitate ad un semplice incarico o a un contesto molto specifico, oppure essere molto generali.

Si tratta, esemplificando, del concetto di esternalizzazione di alcune operazioni di trattamento mediante l'affidamento a terzi, in grado di offrire opportune garanzie: la figura e il ruolo del responsabile, discussa e che presenta molteplici gradazioni, è da sempre al centro di accesi dibattiti ai fini di precisa individuazione. Esemplificando è possibile accennare al fatto che, generalmente, è possibile individuare un soggetto quale responsabile allorché le attività di trattamento affidategli gli siano state delegate da altri, ossia dal titolare, per ragioni di "comodità", speditezza, competenze tecniche e specialistiche particolari ma che, in teoria, avrebbero potuto essere svolte dal titolare stesso[32].

Il rapporto tra il titolare e il responsabile è regolato e precisato nell'**art. 28 del Regolamento**, il quale dispone che la designazione debba avvenire mediante un contratto o un altro atto giuridico con un contenuto minimo perché il responsabile sia concretamente ed effettivamente vincolato al rispetto, nei confronti del titolare, di diversi impegni: la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del titolare del trattamento; devono altresì essere indicate precise istruzioni affinché il responsabile adempia solo agli obblighi impostigli dal titolare.

4.3. AUTORIZZATI AL TRATTAMENTO

Il Regolamento Europeo prevede per il titolare del trattamento l'obbligo di autorizzare e formare gli addetti al trattamento dei dati personali, ossia le persone che, sotto la sua diretta autorità, effettuino operazioni di trattamento.

Mentre l'art. 4, c. 1, lett. h) del Codice Privacy del 2003, oggi abrogato a seguito delle disposizioni contenute nel D.Lgs. 101/2018, contemplava espressamente la presenza e insieme la necessità di individuare, autorizzare e istruire gli

[32] Si veda quanto indicato dall'Autorità Garante Italiana nel noto provvedimento in materia di qualificazione del ruolo dei consulenti del lavoro: la "figura del responsabile, … anche in base alla nuova disciplina pienamente in vigore nel nostro ordinamento a far data dal 25 maggio 2018 rimane connotata dallo svolgimento di attività delegate dal titolare il quale, all'esito di proprie scelte organizzative, può individuare un soggetto particolarmente qualificato allo svolgimento delle stesse (in termini di conoscenze specialistiche, di affidabilità, di struttura posta a disposizione, v. considerando 81, Reg. cit.), delimitando l'ambito delle rispettive attribuzioni e fornendo specifiche istruzioni sui trattamenti da effettuare. Il titolare pertanto è il soggetto che, alla luce del concreto contesto nel quale avviene il trattamento, assume le decisioni di fondo relative a finalità e modalità di un trattamento lecitamente effettuato in base ad uno dei criteri di legittimazione individuati dall'ordinamento (v. artt. 6 e 9 del Regolamento)": https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9081082#3.

"incaricati", ossia le "*persone fisiche autorizzate a compiere operazioni di trattamento*", la formulazione dell'**art. 29** del Reg. Europeo nr. 679/2016, a mente del quale

"il responsabile o chiunque agisca sotto la sua autorità o sotto quella del titolare … che abbia accesso a dati personali non può trattare tali dati se non è ***istruito*** *in tal senso … salvo lo richieda il diritto dell'unione o degli Stati membri*",

aveva fatto sorgere alcuni dubbi sulla compatibilità della menzionata figura degli "incaricati" con il nuovo testo europeo[33].

Tuttavia, proprio la lettura del menzionato art. 29 porta a ritenere che chiunque possa accedere ai dati personali (trattati dal titolare o dal responsabile) debba essere specificamente autorizzato e adeguatamente istruito.

L'**art. 32, 4.**, in tema di sicurezza del trattamento, conferma infatti a chiare lettere che il titolare e il responsabile del trattamento devono far 'sì "*che chiunque agisca sotto la loro autorità e abbia accesso ai dati personali non tratti tali dati se non è istruito in tal senso…*".

Con l'entrata in vigore, a settembre 2018, delle disposizioni di adeguamento del C.P. di cui al D.Lgs. 101/208 e, in particolare, con l'introduzione dell'**art. 2 – *quaterdecies*** nel **D.Lgs. 196/2003**, che prevede l'attribuzione "di funzioni e compiti a **soggetti designati**", gli eventuali dubbi in ordine alla possibilità (o meglio: necessità) di individuare specificamente i soggetti autorizzati al trattamento dei dati personali e di fornire loro specifiche istruzioni, sono svaniti.

4.4. RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Il Regolamento Europeo introduce la figura del Responsabile dei dati personali (RDP: **artt. 37-39**); esso prevede l'obbligo, per il titolare o per il responsabile del trattamento, di designare tale figura:

- *"quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali"* (art. 37, paragrafo 1, lett a);

[33] V. A. D'Ottavio, Ruoli e funzioni privacy principali ai sensi del regolamento: Cap. VI, in *Circolazione e Protezione dei Dati personali, tra Libertà e Regole del Mercato, Commentario al Reg. Eu n. 679/206*, a cura di R. Panetta, Giuffré Francis Lefebvre, 2019, in particolare pagg. 178 e ss..

- *"quando le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala"* (art. 37, paragrafo 1, lett b); oppure
- *"le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10"* (art. 37, paragrafo 1, lett b).

L'Art. 37, paragrafo 2, precisa che *«un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento»*.

Le predette disposizioni prevedono che il RPD *«può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi»* (art. 37, paragrafo 6) e deve essere individuato *«in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui all'articolo 39»* (art. 37, paragrafo 5) *e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento»* (considerando n. 97 del GDPR).

I compiti del Responsabile della Protezione dei Dati sono indicati nell'art. 39 del GDPR:

> "**1.** *Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:*
>
> **a)** *informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;*
>
> **b)** *sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la*

sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) *fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;*

d) *cooperare con l'autorità di controllo; e*

e) *fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.*

2. *Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.*"

5. I PRINCIPI

5.1. L'ART. 5 DEL GDPR

1. *"I dati personali sono*

a) *Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato* (**LICEITA', CORRETTEZZA, TRASPARENZA**)*;*

b) *Raccolti per finalità determinate, esplicite, legittime e successivamente trattati in un modo che non sia incompatibile con tali finalità…* (**LIMITAZIONE DELLA FINALITA'**)*;*

c) *Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono stati trattati* (**MINIMIZZAZIONE DEI DATI**)*;*

d) *Esatti e, se necessario, aggiornati* (**ESATTEZZA**)*; …*

e) *Conservati 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* (**LIMITAZIONE DELLA CONSERVAZIONE**)*; …*

f) *Trattati in maniera da garantire un'adeguata sicurezza … mediante misure tecniche e organizzative adeguate, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione, o dal danno accidentali* (**INTEGRITA' E RISERVATEZZA**).

2. *Il Titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo.* (**ACCOUNTABILITY**)"

Lungi dal costituire mere affermazioni di principio, le previsioni dell'art. 5 del Regolamento Generale sono **i cardini delle nuove disposizioni**.

I principi generali hanno una valenza e una portata davvero ampia, che riguarda ogni aspetto della protezione dei dati, a partire dalla raccolta delle informazioni per passare alle modalità di trattamento e per finire dopo il termine dell'utilizzo dei dati, dopo la cancellazione o la distruzione, come vedremo oltre[34].

[34] I Principi applicabili al trattamento dei dati personali - PRIVACY. Protezione e trattamento dei dati. IPSOA MANUALI – WOLTERS KLUWER, 2020, pagg. 79 e ss..

5.1.1. LICEITA'

Liceità significa che i dati personali devono essere trattati nel rispetto delle norme: un trattamento è lecito allorché non violi norme generali o specifiche dell'Ordinamento. Liceità significa inoltre che, per essere conforme alle norme, il trattamento deve essere effettuato in presenza di una delle condizioni (appunto: di liceità) previste dall'art. 6 del Regolamento, ossia in presenza del consenso dell'interessato o di una delle altre condizioni in esso previste[35].

5.1.2. CORRETTEZZA

Correttezza significa, principalmente, rispetto delle norme etiche, deontologiche e degli accorgimenti necessari a rendere trasparente e comprensibile la relazione tra il titolare del trattamento e l'interessato: i responsabili del trattamento dei dati dovrebbero informare gli interessati e il pubblico in generale del fatto che tratteranno i dati in modo lecito e trasparente e devono essere in grado di dimostrare la conformità delle operazioni di trattamento con il RGPD[36].

5.1.3. TRASPARENZA

Il concetto di trasparenza richiama l'obbligo imposto sul titolare del trattamento affinché ponga in essere misure adeguate e consone per informare gli interessati, siano essi dipendenti, clienti, fornitori o soggetti che chiedano informazioni, sulle modalità con le quali i rispettivi dati personali vengono utilizzati.

Trasparenza significa altresì tracciabilità delle informazioni e dei relativi flussi, documentabilità degli stessi, capacità di rispondere, in modo esaustivo e dettagliato all'interessato che ne faccia richiesta di come e attraverso chi i dati personali vengono trattati: il trattamento deve essere, in tutte le sue fasi, prevedibile e comprensibile, "così da consentire all'interessato il controllo sui propri dati."[37]

5.1.4. LIMITAZIONE DELLE FINALITA'

Gli scopi (*purposes*) del trattamento devono essere determinati, espliciti e legittimi sin dal momento in cui si forniscono le informazioni agli interessati: la finalità del trattamento deve essere definita e comunicata prima che il trattamento abbia inizio; eventuali trattamenti successivi e ulteriori rispetto agli iniziali non devono avere una finalità incompatibile con quella per la quale sono stati iniziati e raccolti[38].

[35] V. al punto successivo: Art. 6: Liceità del trattamento.
[36] Si veda il Manuale Europeo sulla Protezione dei Dati Personali, pag. 132, cit..
[37] Così, nel commento all'art. 5 del Regolamento in Codice di disciplina della Privacy, diretto da L. Bolognini e E. Pelino, Giuffrè Francis Lefebvre, 2019.
[38] Salvo che per l'ulteriore trattamento per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche: art. 5, par. 1, lett. b).

Il principio della limitazione delle finalità significa che qualsiasi trattamento di dati personali deve essere effettuato per una finalità specifica e ben definita e, in caso di scopi ulteriori, solo se specifici e compatibili con la finalità iniziale: le persone, in sostanza, devono sapere cosa aspettarsi dal momento in cui forniranno i propri dati; in tal modo aumenterà anche la possibilità di poter esercitare i diritti allorché lo riterranno opportuno.

Ogni nuova finalità di trattamento che non sia incompatibile con quella originaria deve avere una base giuridica specifica e non può basarsi sul fatto che le informazioni fossero state acquisite inizialmente o trattate per una finalità differente[39].

In tema di limitazione delle finalità è essenziale il contributo del Gruppo di lavoro dei 29 (ex WP 29) e quanto evidenziato nell'*Opinion 3/2013 on purpose limitation*, che suddivide il tema sotto due aspetti. Il primo è quello, sostanzialmente, della individuazione della esplicita finalità dichiarata agli interessati e che consente di dar loro completa comprensione del quadro sostanziale di riferimento; il secondo è quello dei trattamenti successivi e ulteriori rispetto alla finalità originaria e, quindi, quello del riuso[40].

5.1.5. MINIMIZZAZIONE DEI DATI

Il trattamento dei dati personali deve essere limitato a quanto necessario per perseguire una finalità legittima e il trattamento può essere effettuato se tale finalità non è ragionevolmente perseguibile con altri mezzi. Il trattamento, inoltre, non deve interferire in modo sproporzionato con gli interessi, i diritti e le libertà dell'interessato.

Il principio in discorso è l'espressione dei principi di adeguatezza, pertinenza e necessità rispetto alle finalità e strettamente connesso ai principi di responsabilizzazione, *privacy by design* e *by default* che esamineremo successivamente.

Esso ha una portata generale, perché implica la necessità di ridurre al minimo il numero e la tipologia dei dati trattati, le tipologie e modalità di trattamento, dei soggetti che hanno accesso alle informazioni, delle tempistiche di conservazione.

Con l'utilizzo delle nuove tecnologie è possibile ridurre al minimo e finanche, talvolta, evitare l'utilizzo dei dati personali o utilizzare misure per ridurre la

[39] Uno dei temi di maggiore rilevanza sollevato dal principio di limitazione delle finalità è quello dei dati inferiti, ossia degli *inferred data*: le odierne tecnologie consentono di ricavare dati da altri dati e, in tal modo, di prevedere le preferenze degli interessati. Per interessanti approfondimenti e segnalazioni sui pericoli di tali sviluppi, si veda F. PIZZETTI, su Agenda Digitale, 13 luglio 2018: https://www.agendadigitale.eu/sicurezza/portabilita-dei-dati-nel-gdpr-cosa-significa-e-cosa-implica-questo-nuovo-diritto/ .

[40] https://www.garanteprivacy.it/documents/10160/2133805/WP203+Parere+su+principio+di+finalit%C3%A0.pdf/8d300b14-dccf-4069-a2f9-bff5c52df526?version=1.3.

capacità di attribuire i dati a specifici interessati, per esempio utilizzando la tecnica della pseudonimizzazione[41].

5.1.6. ESATTEZZA

I dati devono essere esatti e, se necessario, aggiornati, adottando ragionevoli ma adeguate misure al fine di cancellare o rettificare con tempestività eventuali informazioni inesatte.

In tale concetto rientrano certamente anche quello di aggiornamento di dati non più corretti e quello di integrazione delle informazioni eventualmente divenute incomplete: può essere necessario controllare i dati periodicamente e regolarmente, aggiornandoli ove necessario.

Può del resto accadere che vi siano "situazioni in cui il controllo regolare dell'esattezza dei dati, fra cui l'aggiornamento, costituisce una necessità assoluta", a motivo del potenziale danno che ne potrebbe derivare all'interessato qualora i dati dovessero essere inesatti[42].

5.1.7. LIMITAZIONE DELLA CONSERVAZIONE

I dati personali devono essere cancellati o resi anonimi (anonimizzati) allorché non siano più necessari per le finalità per le quali sono stati raccolti.

Il Considerando 39 del Regolamento precisa che "il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica" al fine di garantire che i dati non siano conservati più a lungo del necessario.

5.1.8. INTEGRITA' E RISERVATEZZA LA SICUREZZA

Sicurezza e riservatezza sono fondamentali al fine di prevenire effetti negativi per gli interessati.

I dati devono essere trattati mediante adeguate misure protettive, tecniche ma anche organizzative, al fine di prevedere accessi o, in ogni caso, trattamenti non autorizzati o illeciti, nonché al fine di prevenirne l'eventuale uso, consultazione, manomissione, perdita, distruzione o danneggiamento, illegali o anche solo accidentali.

Diretta e conseguente applicazione del principio in discorso è l'**art. 32** del Regolamento, "**Sicurezza del trattamento**", che dispone espressamente che

"*tenuto conto*

- *dello stato dell'arte,*
- *dei costi di attuazione, nonché*

[41] Si veda il Manuale Europeo sulla Protezione dei Dati Personali, pag. 141: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_it.pdf.
[42] Manuale Europeo sulla Protezione dei Dati, pag. 143.

- *della natura,*
- *dell'oggetto,*
- *del contesto e*
- *delle finalità del trattamento, come anche*
- *del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche,*

il titolare del trattamento e il responsabile del trattamento ***mettono in atto misure tecniche e organizzative adeguate*** *per garantire un livello di sicurezza adeguato al rischio.*"

Il principio della sicurezza del trattamento[43], uno dei cardini della normativa europea, è intimamente collegato, come si vedrà, ai principi della responsabilizzazione (art. 24) e della privacy *by design* e *by default* (art. 25): è lo stesso articolo 5, paragrafo 2, del GDPR a introdurre ed esplicitare l'accountability, laddove precisa e impone al titolare di essere in grado di dimostrare di avere rispettato i principi generali.

5.2. L'ART. 6 del GDPR

LICEITA' DEL TRATTAMENTO

Il trattamento è lecito se e nella misura in cui ricorra almeno una delle seguenti condizioni:

a) L'interessato ha espresso il proprio **consenso**;

b) Il trattamento è necessario per l'esecuzione di un **contratto** di cui l'interessato è parte o per l'esecuzione di misure precontrattuali adottate su richiesta dell'interessato:

c) Il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) Il trattamento è necessario per la **salvaguardia di interessi vitali** dell'interessato o di un'altra persona fisica;

e) Il trattamento è necessario per **l'esecuzione di un compito di interesse pubblico** o connesso all'**esercizio di pubblici poteri** di cui è investito il titolare del trattamento;

f) Il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli

[43] Per il quale si rimanda, più diffusamente, alle previsioni dell'art. 32 del GDPR.

interessi o i diritti fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore[44].

Come si vede, l'art. 6 elenca le basi giuridiche di liceità del trattamento, ovvero le condizioni alle quali può dirsi che il trattamento dei dati personali avvenga nel rispetto delle norme.

Si noti come sia **precisa scelta** del legislatore europeo **non attribuire ad alcuna delle condizioni** che esamineremo assai succintamente qui di seguito, **rilevanza o preminenza**: non è infatti indicata "una condizione su cui sia preferibile fondare il trattamento[45]".

5.2.1.1. CONSENSO

La prima condizione di liceità del trattamento è data dalla manifestazione del consenso da parte dell'interessato[46].

Il consenso al trattamento dei dati personali deve essere volontario, consapevole, informato, specifico, inequivocabile e deve essere manifestato con una azione esplicita e "positiva"[47]. Resta inteso che il consenso è relativo al trattamento dei dati personali e non al rapporto sostanziale tra le parti.

Quel che principalmente mette conto sottolineare è che il consenso debba essere prestato con azioni positive, ossia con una dichiarazione scritta, con una dichiarazione verbale registrata, con azioni fisiche e, soprattutto, che debba essere informato, in relazione, almeno, all'identità del titolare e alle finalità del trattamento[48]. Se l'interessato non è in grado di optare per una scelta autenticamente libera, l'eventuale consenso non potrà dirsi liberamente prestato o espresso.

Nel contesto di una dichiarazione scritta che riguardi anche altre questioni, come avviene allorché siano presentate condizioni e termini di un servizio, la richiesta di manifestazione del consenso deve essere presentata con un linguaggio semplice e chiaro, in forma comprensibile e facilmente accessibile, in modo che sia chiara la distinzione tra esso e altre questioni.

---

[44] Questa ultima disposizione, art. 6 lett. f), non si applica allorché il trattamento sia effettuato da autorità pubbliche nell'esecuzione dei relativi compiti. In base, inoltre, alle previsioni dellart. 6, par. 2, gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme ai trattamenti necessari per adempiere un obbligo legale cui è soggetto il titolare o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare.

[45] Commento all'art. 6 del Regolamento in Codice di disciplina della Privacy, diretto da L. Bolognini e E. Pelino, Giuffrè Francis Lefebvre, 2019, pag. 92.

[46] Si vedano, al riguardo, le Linee Guida del WP 29 sul consenso: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, nonché quelle sulla trasparenza: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[47] V. il Manuale Europeo sulla Protezione dei Dati, cit. pag. 126.

[48] Le citate Linee Guida su consenso precisano che l'interessato debba conoscere, ai fini di una positiva manifestazione, non solo l'identità del titolare e le finalità per le quali il consenso è richiesto, ma anche quali tipi di dati siano raccolti, l'esistenza del diritto di revocare il proprio consenso, le informazioni sull'esistenza di un processo decisionale automatizzato, le informazioni sui possibili rischi di trasferimenti di dati in Paesi extra Ue.

E’ opportuno rammentare come, ai sensi dell’art. 7 del Regolamento, il titolare abbia l’onere di dimostrare la prestazione del consenso da parte dell’interessato.

5.2.2.CONTRATTO

Il trattamento dei dati personali è lecito allorché esso sia necessario all’esecuzione di un contratto del quale l’interessato sia parte, come avviene, ad esempio, per il trattamento di dati personali del lavoratore quali retribuzioni, dati bancari, dati fiscali, finalizzati al pagamento dello stipendio; per il trattamento dei dati di contatto e di residenza di un acquirente di un bene on-line; dei dati della carta di credito per il pagamento di un servizio acquistato.

Si badi, ovviamente, che il titolare non sia per ciò stesso legittimato a trattare ogni genere o tipo di dati personali del soggetto con il quale ha in corso un rapporto contrattuale: egli potrà e dovrà trattare solo quelli realmente e strettamente necessari all’esecuzione dello stesso in relazione alle specifiche obbligazioni assunte.

Si noti come la condizione di liceità sia estesa all’esecuzione delle prestazioni precontrattuali, allorché è evidente come, ad esempio, sia necessario trattare dati personali identificativi di contatto (nome, indirizzo, ecc.), per inviare un preventivo.

5.2.3.OBBLIGO LEGALE

Come evidente, la sussistenza di un obbligo legale esime il titolare e lo legittima al trattamento di dati personali, come avviene ad esempio nel trattamento relativo all’adempimento degli obblighi antiriciclaggio, di tutta la normativa fiscale, di altri obblighi imposti ai titolari, come le comunicazioni di versamenti e altre incombenze sui datori di lavoro nei confronti del proprio personale.

5.2.4. INTERESSE VITALE

Del pari evidente come la salvaguardia di un bene supremo come quello relativo agli interessi vitali di un interessato esima il titolare dalla ricerca di una diversa condizione di liceità come potrebbe essere il consenso.

La condizione è applicabile solo se nessuna delle altre lo sia, come avviene ad esempio nel caso delle emergenze umanitarie.

5.2.5.PUBBLICO INTERESSE e PUBBLICI POTERI

Nel settore delle Pubbliche Amministrazioni e degli altri titolari che operano nel pubblico interesse la base normativa sostituisce ed esaurisce gli altri presupposti.

5.2.6. LEGITTIMO INTERESSE

Esaminando brevemente la condizione di liceità prevista dalla lettera f) dell'art. 6, par. 1, vale la pena evidenziare come, affinché si possa basare il trattamento sul legittimo interesse del titolare o di terzi, è necessario che il trattamento sia:

- Funzionale al raggiungimento della finalità legittima perseguita,
- Sufficientemente articolato da permettere il test di bilanciamento, da effettuare di volta in volta, caso per caso, con l'interesse o i diritti fondamentali dell'interessato, in particolare ove questi sia un minore,
- Reale ed attuale, ovvero corrisponda a un beneficio atteso in un futuro prossimo[49].
- Si può inoltre affermare che il legittimo interesse, per costituire una base giuridica idonea (lecita) deve prevalere sui diritti e sulle libertà fondamentali degli interessati[50].

Il Gruppo di lavoro dei Garanti Europei ha evidenziato, in particolare, come nell'effettuare il test di bilanciamento (legittimo interesse / interessi – diritti del soggetto) si debbano tenere in considerazione:

a) La natura del legittimo interesse e in particolare la necessità del trattamento e la sua proporzionalità rispetto al diritto fondamentale in gioco;
b) Gli impatti sull'interessato e la ragionevole aspettativa su quanto possa accadere in relazione ai suoi dati personali tenendo conto della natura degli interessi e delle modalità di trattamento;
c) Le eventuali misure di sicurezza addizionali adottate per tali trattamenti.

Mentre il Regolamento non fornisce un elenco di casi espliciti di legittimo interesse, nei Considerando vi sono alcuni esempi di legittimo interesse: il Considerando 47 ritiene possa sussistere la condizione di liceità in discorso laddove esista una relazione pertinente e appropriata tra l'interessato e il titolare, come avviene per esempio allorché l'interessato sia un cliente o un dipendente del titolare; ulteriormente, può essere considerato presente il legittimo interesse laddove il titolare intenda trattare dati personali strettamente necessari ai fini di prevenzione delle frodi; suscitando accesi dibattiti, inoltre, il Considerando in questione ritiene sussistente il legittimo interesse laddove il titolare tratti dati personali a fini di *marketing* diretto. Il Considerando 48 ritiene sussistente il legittimo interesse nell'ipotesi di trasmissione di dati personali all'interno di un gruppo imprenditoriale a fini amministrativi e il Considerando 49 per le ipotesi in cui sia necessario trattare

[49] Importanti e interessanti indicazioni sul concetto di interesse legittimo sono rinvenibili nel parere dell'ex Gruppo dei 29 (WP29) adottato il 9 aprile 2014: *Opinion 6/2014, legitimate interest*, qui nella versione in lingua italiana: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.
[50] Dati e trattamenti - PRIVACY. Protezione e trattamento dei dati, cit. pag. 114.

dati personali relativi al traffico in rete, in misura strettamente necessaria e proporzionale a garantirne la sicurezza della stessa e dell'informazione[51].

5.3. L'ART. 24 del GDPR

L'ACCOUNTABILITY

Il principale strumento utilizzato dal Legislatore europeo per operare un deciso cambio di prospettiva nell'ambito della tutela e protezione dei singoli individui in relazione al trattamento dei loro dati personali è costituito dal principio della *accountability*[52].

La responsabilizzazione richiede ai titolari e ai responsabili del trattamento dei dati personali di adottare, in modo attivo (pro – attivo) e continuo, misure finalizzate alla protezione e salvaguardia delle informazioni (dei dati) non solo nella fase del trattamento vero e proprio, ma anche nella fase della progettazione dello stesso.

Come già evidenziato, i titolari devono essere in grado di dimostrare in qualsiasi momento agli interessati e alle Autorità di controllo che essi operano conformemente alle norme e alle disposizioni.

Senza entrare nello specifico di alcune differenze terminologiche che si trovano nei testi inglese ed italiano del GDPR in relazione alla traduzione del termine responsabilità o responsabilizzazione[53], basti qui rilevare come il termine *accountability* richiami, quanto meno, due accezioni o componenti essenziali:

a) In primo luogo l'essere in grado di **dare conto e giustificazione**, all'esterno, in modo completo e dettagliato, "del corretto utilizzo delle risorse e della produzione di risultati in linea con gli scopi istituzionali" e,

b) In secondo luogo "l'esigenza di **introdurre logiche e meccanismi di maggiore responsabilizzazione interna** alle aziende … relativamente all'impiego di tali risorse e alla produzione dei correlati risultati."[54]

Tale responsabilizzazione assume la veste della

---

[51] Si veda, con maggiore dettaglio, il commento all'art. 6, par. 1, lett. f) in L. BOLOGNINI, *Commentario al Reg. UE n. 2016/679 e al novellato d.lgs. 196/2003*, Giuffrè Francis Lefebvre, 2019, pag. 96 nonché Dati e trattamenti - PRIVACY. Protezione e trattamento dei dati. IPSOA MANUALI – WOLTERS KLUWER, 2020, pagg. 114 e ss..

[52] Si veda, al riguardo, il Parere 3/2010 del WP 29 sul principio di responsabilità: https://www.garanteprivacy.it/documents/10160/10704/Articolo+29+-+WP173+-+Parere+3+2010+sul+principio+di+responsabilit%C3%A0.pdf/006f43b3-7180-4485-903e-bf8b4f367763?version=1.2.
Anche il Considerando 74 del Regolamento prevede che sia opportuno stabilire la responsabilità generale del titolare affinché sia tenuto a mettere in atto misure adeguate ed efficaci e che sia in grado di dimostrare la conformità delle proprie attività di trattamento, compresa l'efficacia delle stesse.

[53] In relazione alle quali è possibile approfondire l'argomento in N. FABIANO, *GDPR & Privacy, Consapevolezza e opportunità*, goWare, Firenze, 2019, pagg. 25 e ss..

[54] M. IASELLI, *Manuale operativo del D.P.O.*, Maggioli Editore,2018, pag. 9.

➔ **trasparenza**, intesa come garanzia di accessibilità alle informazioni e al modus operandi del titolare del trattamento o del responsabile; della

➔ **responsività** in relazione alle scelte organizzative, gestionali, operative e procedurali messe in atto nonché della

➔ ***compliance***, intesa come capacità di rispettare e far rispettare le norme e le regole di comportamento esistenti.

Ben si può dire, pertanto, che il principio dell'accountability, cristallizzato **nell'art. 24 del GDPR**, scolpisca uno "dei principi fondamentali e tra i più innovativi del Regolamento, l'essenza del cambiamento di approccio del legislatore"[55]: è infatti compito del titolare del trattamento,

"*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà fondamentali delle persone fisiche,*" ***mettere "in atto*** *misure tecniche e organizzative adeguate per garantire,* ***ed essere in grado di dimostrare****, che il trattamento è effettuato conformemente al presente regolamento.*"

La "responsabilizzazione" del titolare (ma anche del responsabile del trattamento) impone a chiunque tratti dati personali di essere dunque *accountable*, ossia non solo

➔ **responsabile delle procedure**, **delle scelte operate** per la realizzazione delle proprie attività che comportino il trattamento di dati personali, ma anche e soprattutto di essere

➔ **in grado di** riferire e **chiarire, con trasparenza, agli interessati, le scelte** che li coinvolgano e, non per ultimo, di

➔ **documentare** scelte, processi e decisioni **all'Autorità** di controllo che dovesse chiederne conto[56].

Il profilo della "responsabilizzazione" si coglie anche dall'esame del concetto di "adeguatezza" delle misure adottate, in assenza di specifiche, ormai abrogate, indicazioni[57]: il titolare dovrà dunque dimostrare, all'occorrenza, di avere

---

[55] F. CAPPARELLI, commento all'art. 24 in Codice di disciplina della Privacy, diretto da L. Bolognini e E. Pelino, Giuffrè Francis Lefebvre, 2019.

[56] Obbligo visto alla luce della doppia accezione di "Responsabilizzazione" e "rendicontazione": Codice di disciplina della Privacy, cit., pag. 88.

[57] Il riferimento è all'abrogazione, avvenuta con il d.lgs. 101/2028, dell'Allegato B del Codice Privacy di cui al d.lgs. 196/2003, ossia delle Misure Minime Obbligatorie, il disciplinare tecnico in base al quale, sostanzialmente, per assicurare la conformità alla normativa in relazione ai dati trattati, era sufficiente porre in essere le indicazioni fornite nell'allegato in questione, il che si tramutava, nei fatti, nella mera "dotazione" di un elenco nominativo e nell'esecuzione di pochi e semplici controlli, tipo il back up periodico e il cambio delle password. Il progresso tecnologico e la differente natura e

adottato delle misure che, preso atto di quanto indicato nell'art. 24 (natura, ambito di applicazione, contesto e finalità del trattamento ma anche rischi) si dimostrino adeguate alla tutela e protezione dei dati degli interessati.

Ma non solo, giacché i titolari del trattamento dovranno anche dimostrare di essere *compliant* con le norme, seguendone le imposizioni e, pertanto, adottare, porre in essere, disporre le misure e le procedure previste, di volta in volta, dal Regolamento e dalle disposizioni loro applicabili[58].

Di fatto, il principio in esame rovescia la prospettiva in tema di protezione dei dati personali ponendo, in capo ai titolari e in certa misura ai responsabili, il dovere di responsabilizzarsi: il titolare, quale soggetto che determina le finalità e i mezzi del trattamento, trova, in tale propria discrezionalità, da adeguare ai casi concreti ed effettivi, anche il "limite" o, se si vuole, l'opportunità, di conformare la propria attività nel modo più confacente al caso di specie, ma ha l'onere di dimostrare le ragioni a supporto delle proprie decisioni e le motivazioni che lo hanno portato a ritenere le proprie scelte *compliant* rispetto alle norme.

5.4. L'ART. 25 DEL GDPR

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

L'art. 25 del Regolamento, insieme al Considerando 78, impone ai titolari che intendano progettare processi e servizi che implicano il trattamento di dati personali di attribuire alle norme in materia di protezione delle informazioni rilevanza e, in un certo senso, precedenza in tutte le fasi, a partire da quella di "ideazione di nuovi processi e servizi"[59].

In questo senso il titolare del trattamento deve fare in modo di **attuare la protezione dei dati personali** e delle informazioni sin dal momento in cui predispone la propria organizzazione in tal senso e, successivamente, in ogni momento in cui avviene il trattamento stesso.

Egli deve quindi **organizzarsi e adottare sistemi, apparecchi e applicazioni che siano stati pensati e progettati tenendo presente la disciplina, gli obblighi e i doveri in materia di trattamento dei dati**.

Egli deve, ulteriormente, **dotarsi di procedure, modelli organizzativi e protocolli pensati per proteggere i dati che tratta**. Se necessario egli deve implementare tali procedure e, in ogni caso, tenerle aggiornate e verificarne

ambito di operatività delle moderne realtà industriali e commerciali *data based* hanno reso obsoleta e poco efficace una tale impostazione.

[58] Il riferimento è, ad esempio, alla tenuta del registro delle attività di trattamento (art. 30), alla designazione, ove necessario, del Responsabile della Protezione dei Dati (art. 37), alla valutazione di impatto (art. 35), a prevedere modalità di riscontro ai diritti dell'interessato (art. 12), alla revisione di processi, procedure e modalità, ecc..

[59] V. il commento all'art. 25 in Codice di disciplina della Privacy, diretto da L. Bolognini e E. Pelino, Giuffrè Francis Lefebvre, 2019, pag. 203.

l'adeguatezza al contesto, alla natura del trattamento e alle finalità per le quali le informazioni vengono trattate.

5.4.1. PRIVACY BY DESIGN

Protezione dei dati fin dalla progettazione

L'art. 25, paragrafo 1 dispone:

"*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,* ***sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento*** *stesso il titolare del trattamento* ***mette in atto misure tecniche e organizzative adeguate****, quali la pseudonimizzazione,* ***volte ad attuare in modo efficace i principi di protezione dei dati****, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*"

Fin dal momento della progettazione di un sistema, di un processo, di un applicativo, di una procedura, di una modalità di trattamento dei dati personali è imprescindibile tenere in considerazione la necessità di protezione dei dati personali: i titolari e i responsabili del trattamento devono aver riguardo e valutare, prima di iniziare l'attività di trattamento, il probabile effetto che questo potrà avere sui diritti e sulle libertà delle persone fisiche. Essi devono **progettare i sistemi al fine di** evitare il più possibile e in ogni caso **minimizzare** (minimizzazione) **il trattamento**, **di modo che i rischi** di ingerenza nei diritti e nelle libertà degli interessati **siano ridotti al minimo**.

In sostanza, il trattamento deve essere pensato e progettato, sin dall'origine e quindi dal relativo sviluppo, ai fini di maggior tutela possibile degli interessati.

I criteri e i parametri che consentono tali valutazioni sono indicati all'inizio del paragrafo che stiamo esaminando: lo stato dell'arte, i costi di attuazione, la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, la probabilità e la gravità dei rischi per gli interessati: si tratta di operare una analisi di sostenibilità "da cui può emergere un'originale combinazione di misure tecniche e misure organizzative"[60].

E' così possibile operare valutazioni di tipo tecnologico (esistono tecnologie, sistemi, applicativi in grado di proteggere le informazioni?), di tipo fattuale sulla tipologia di attività che devono essere svolte (quale tipologia di attività viene svolta? Con quali tipologie di dati personali, comuni o di tipo particolare? Essa

[60] PRIVACY. Protezione e trattamento dei dati. IPSOA MANUALI – WOLTERS KLUWER, 2020, pagg. 271 e ss.

viene effettuata per dare seguito a un rapporto contrattuale o sulla base di un legittimo interesse del titolare? Si tratta di una attività svolta nell'esercizio di un'attività imprenditoriale o di tipo pubblicistico?) ovvero esaminare la probabilità e la gravità dei rischi che le persone potrebbero dover affrontare.

In generale è possibile evidenziare, in ogni caso, che la protezione dei dati personali ai fini del rispetto delle prescrizioni del Regolamento può essere affrontata e risolta mediante l'adozione di misure tecniche e mediante misure organizzative.

5.4.1. a) Misure organizzative

E' certamente vero che nella precedente normativa in materia di protezione dei dati personali le misure atte a regolamentare i flussi e le procedure di dati e informazioni all'interno delle organizzazioni avevano precipua rilevanza.

Oggi, tuttavia, risulta oltremodo necessario predisporre **policy e procedure interne all'organizzazione** volte a prevenire incidenti di sicurezza e violazioni di dati personali[61]. Il cambio di passo è però, di fatto, dato dalla rilevanza più sostanziale che meramente "burocratica" della presenza di tali procedure, basti rilevare che le attività ispettive sino ad oggi espletate in tutta Europa hanno posto l'accento, più che sulla forma, sulla sostanza, ossia sulla reale rispondenza al vero e a quanto viene svolto in azienda dal titolare che non a quanto, seppur analiticamente, indicato nelle comunque necessarie procedure organizzative predisposte[62].

È essenziale **minimizzare le attività di trattamento** allo stretto necessario, così come, ancor prima, minimizzare tipologia e numero di informazioni da trattare allo stretto necessario, in relazione ovviamente alle finalità che si perseguono.

E' altresì necessario prevedere e organizzare internamente le aziende mediante **precise attribuzioni di ruoli e, sovente, di profili di autorizzazione**. È necessario e imprescindibile autorizzare il personale e i dipendenti e periodicamente effettuare sessioni di formazione e aggiornamento.

L'esistenza di norme che impongono al titolare di segnalare (*rectius*: di notificare all'Autorità Garante ed eventualmente di comunicare al diretto interessato[63]) l'avvenuta violazione delle informazioni, impone al titolare di prevedere e mettere in atto misure organizzative non solo volte a evitare tali accadimenti ma anche a rispondere prontamente ogni qualvolta ciò dovesse avvenire. Il che è possibile solo laddove esistano modelli organizzativi chiari e precisi sulle attribuzioni di funzioni e compiti nelle diverse circostanze.

---

[61] Si vedano le interessanti e utili indicazioni di G. Ziccardi, *GDPR e set di istruzioni per i soggetti che trattano dati: l'uso degli strumenti informatici, la gestione di possibili data breach e la protezione dal phishing*, in Diritto di Internet, 1/2019, pagg. 223 e ss., Pacini Giuridica.

[62] https://zerodays.podbean.com/e/una-policy-gdpr-in-previsione-delle-sanzioni/.

[63] Vedi gli artt. 33 e 34 del Regolamento.

L'alto numero e la particolarità dei diritti riconosciuti agli interessati impongono al titolare, anche in base alle previsioni di cui all'art. 11 del Regolamento, di impostare e prevedere celeri modalità di riscontro agli stessi[64].

5.4.1. b) Misure tecniche

Le indicazioni e le procedure operative da seguire in tema di progettazione di **prodotti e servizi, soprattutto di tipo tecnologico e informatico** che abbiano quale punto di ispirazione e faro ispiratore la **protezione dei dati** personali sono molteplici e varie.

Vale la pena qui brevemente evidenziare i principi formulati dall'agenzia europea ENISA, centro di consulenza per la sicurezza informatica in Europa[65], che ha evidenziato l'importanza di sottolineare e perseguire i seguenti canoni e principi: minimizzare, nascondere, separare, aggregare, informare, controllare, forzare e dimostrare", in sede di progettazione, al fine di ottenere la massima tutela possibile nella ideazione e realizzazione dei progetti e dei servizi tecnologici[66].

5.4.2. PRIVACY BY DEFAULT

Protezione dei dati per impostazione predefinita

Il paragrafo 2. dell'art. 25 descrive il secondo dei principi che stiamo esaminando:

> "*Il titolare del trattamento mette in atto* ***misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari*** *per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.*"

Le misure che il titolare deve adottare impongono di fare in modo che siano trattati (e che pertanto si debba, in qualche modo "forzare il sistema" per operare diversamente) solo i dati strettamente necessari allo scopo e che il rispetto di tale principio sia presente in ogni fase del trattamento. La protezione del dato personale, in altre parole, diviene componente "naturale" delle operazioni di trattamento, sempre tenuta in considerazione.

---

[64] Diverse sanzioni comminate dalle Autorità Garanti europee nel corso del 2019 hanno riguardato la mancata, incompleta, insufficiente risposta del titolare alle richieste di informazioni dell'interessato. Il riferimento normativo è, evidentemente, al citato art. 11 ma anche agli articoli da 15 a 22 e 34 del Regolamento.
[65] https://europa.eu/european-union/about-eu/agencies/enisa_it.
[66] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

Il titolare deve mettere in atto misure adeguate per garantire che siano trattati solo i dati effettivamente necessari ai fini del trattamento e tale obbligo vale per la quantità dei dati trattati, la portata del trattamento, il periodo di conservazione, l'accessibilità agli stessi. Ad esempio, non tutti i dipendenti di un titolare dovrebbero avere accesso ai dati personali degli interessati, ma solo coloro per i quali sia indispensabile avervi accesso ai fini del trattamento stesso[67]
.

Le misure devono fare in modo che non sia possibile accedere alle informazioni (se non "forzando" il sistema) alle persone non debitamente autorizzate; deve esservi sempre un intervento non automatizzato (e quindi umano) nella raccolta dei dati e nella compilazione dei campi.

E' di immediata evidenza l'importanza e la rilevanza che un tale principio ha oggigiorno: le molteplici applicazioni e i diversi servizi, soprattutto della società dell'informazione (il web) devono essere progettati e utilizzabili solo mediante sistemi e procedure contenenti misure di sicurezza aggiornate e allo stato dell'arte.

E' altrettanto evidente le necessità di sistemi di autenticazione "robusti" e di autenticazione a più fattori[68].

6. I DIRITTI DELL'INTERESSATO (CENNI)

Il Regolamento Europeo pone molta enfasi sui diritti degli interessati e, in particolare, sul fatto che ognuno di essi (ciascuno di noi!) abbia il diritto, soprattutto e in primo luogo, di essere informato sul trattamento dei propri dati personali da parte di chiunque lo operi, ossia da parte di ogni e qualsiasi titolare del trattamento, salve poche eccezioni.

Gli interessati, in particolare, hanno diritto di

- Accedere ai propri dati e ottenere determinate informazioni sul trattamento;
- ottenere, se del caso, la rettifica dei propri dati laddove inesatti;

[67] Nel 2016 l'ENISA ha pubblicato una relazione sugli strumenti e sui servizi in materia di vita privata attualmente disponibili489. Tra le altre considerazioni, tale valutazione fornisce un indice di criteri e parametri che sono indicatori di buone o cattive pratiche in materia di riservatezza: Manuale Europeo sulla protezione dei dati, 2018, cit., pag. 206.

[68] Il tema in discorso è quello della generazione delle identità, solitamente attraverso la combinazione dei seguenti fattori:

- una cosa che sai;
- una cosa che hai;
- una cosa che sei.

La combinazione di due fattori genera le cosiddette "credenziali di accesso" al sistema. L'identificazione solitamente è costituita da un codice, spesso scelto direttamente dall'utente. La scelta spesso è effettuata mediante l'utilizzo di nome e cognome, di un soprannome o di un codice; si tratta comunque di un dato da "memorizzare", riguarda il fattore della conoscenza. Con l'account si identifica una persona, la quale attraverso un altro codice, generalmente chiamato password, viene autenticata. Anche la password è da "memorizzare" e di conseguenza afferisce al medesimo fattore: si definisce questa metodologia come un'autenticazione debole. L'utilizzo della combinazione di due fattori (*Strong Customer Authentication*) incrementa la certezza sulla persona che sta accedendo al sistema, perché vengono utilizzati due criteri, la conoscenze e il possesso (qualcosa che hai), mediante l'utilizzo di un *device* (es: *token*) per la ricezione o la generazione di un codice da utilizzare nel processo e utilizzabile una sola volta (come nel caso dell'OTP: *One Time Password*).

- ottenere eventualmente la cancellazione di dati ove il trattamento sia illegittimo;
- limitare temporaneamente il trattamento;
- ottenere il trasferimento dei propri dati a un altro titolare in determinate condizioni.

Gli interessati, inoltre, hanno il diritto di

- opporsi al trattamento dei propri dati per motivi che riguardano la loro situazione particolare, ovvero i loro dati siano utilizzati per il c.d. marketing diretto.

Gli interessati, ancora, hanno il diritto di

- non essere sottoposti a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, e che producano effetti giuridici nei loro confronti o che li riguardino o incidano significativamente sulla loro persona. Gli interessati hanno diritto di ottenere l'intervento umano da parte del titolare e di esprimere la loro opinione e contestare una decisione fondata su un trattamento automatizzato.

In determinate ipotesi gli interessati hanno

- il diritto di essere avvertiti dal titolare ove vi sia stato un incidente che abbia causato la perdita di riservatezza, integrità o disponibilità delle informazioni che li riguardano.

6.1. Diritto ad essere informati

Il titolare del trattamento è obbligato a informare l'interessato, prima ancora dell'operazione di trattamento circa le finalità dello stesso e relativamente a tutto quanto previsto dagli artt. 13 e 14 del Regolamento: l'obbligo non è soggetto ad una eventuale richiesta dell'interessato, ma sussiste per il solo fatto della possibile raccolta di informazioni.

Gli **articoli 13 e 14 del GDPR** precisano, in particolare, le dettagliate "Informazioni" che devono essere rese allorché i dati siano raccolti direttamente dall'interessato (art. 13) oppure in situazioni in cui i dati non siano stati ottenuti direttamente dagli stessi (e, quindi, ricevuti da altri: art. 14).

6.2. Diritto di proporre reclamo

Il Regolamento prevede espressamente, tra le informazioni da fornire all'interessato, quella per la quale egli ha diritto di presentare un reclamo ad una Autorità di Controllo (Garante) e, ove ritenuto necessario, all'autorità Giudiziaria ordinaria, in merito ad una violazione relativa ai propri dati personali. Esistono, peraltro, limitazioni a tale diritto e un certo margine di discrezionalità attribuito agli Stati membri[69].

6.3. Diritto di accesso

[69] Per approfondimenti su questi temi si veda il Manuale Europeo già citato, alle pagg. 238 e ss..

Ai sensi dell'art. 15 del Regolamento ogni interessato ha diritto di ottenere dal titolare informazioni sul trattamento dei propri dati, quali ad esempio: le finalità, le categorie, i destinatari (anche per categorie), il periodo di conservazione, l'esistenza del diritto di rettificare i dati inesatti, come già visto, il diritto di proporre reclamo ovvero, nel caso di decisioni automatizzate, la logica applicata a tali processi[70].

6.4. Diritto di rettifica

Gli interessati hanno diritto di ottenere la rettifica dei loro dati che siano inesatti, inattuali, non corretti.

6.5. Diritto alla cancellazione (oblio)

Si tratta di un diritto particolarmente importante e con implicazioni delicate seppure estremamente interessanti, oggetto di un'ampia letteratura e di molti contributi. L'art. 17 precisa condizioni e limiti per l'esercizio di tale diritto[71].

6.5. Diritto di limitazione del trattamento

L'art. 18 del GDPR autorizza gli interessati a ottenere una provvisoria "interruzione" del trattamento allorquando sia contestata l'esattezza dei dati personali, ovvero che il trattamento sia illecito, i dati debbano essere conservati per l'utilizzo in sede giudiziaria oppure sia pendente una decisione in merito all'eventuale prevalenza dei motivi legittimi del titolare rispetto a quelli dell'interessato.

6.7. Diritto alla portabilità

In base a tale diritto, di nuova introduzione nel campo della protezione dei dati personali, gli interessati hanno diritto di ottenere la trasmissione dei propri dati personali da un titolare del trattamento ad un altro, se ciò sia tecnicamente fattibile, in un formato strutturato e facilmente leggibile da dispositivo elettronico.

6.8. Diritto di opposizione

Il tema è vasto, di estrema attualità e certamente interessante, riguardando sia un'eventuale situazione particolare dell'interessato, sia il c.d. marketing diretto, sia il trattamento mediante mezzi automatizzati, sia l'eventuale obiezione per finalità di ricerca scientifica o storica o per fini statistici.

6.9 Processo decisionale automatizzato, compresa la profilazione: cenni.

[70] Si veda D. MONTANARO, in *Commentario al Reg. UE n. 2016/679 e al novellato d.lgs. 196/2003*, a cura di R. PANETTA Giuffrè Francis Lefebvre, 2019, anche per gli altri diritti, alle pagg. 185 e ss..
[71] V. il commento all'articolo in questione in Codice di disciplina della Privacy, diretto da L. Bolognini e E. Pelino, Giuffrè Francis Lefebvre, 2019.

Il tema della possibile sottoposizione degli interessati a decisioni automatizzate che abbiano effetti giuridici nei confronti degli stessi è estremamente delicato e rilevante. Basti pensare alla possibilità dell'utilizzo degli algoritmi nell'analisi di una mole sempre più significativa di informazioni e alla possibilità di predeterminare ipotesi e possibili risultati analizzando comportamenti, abitudini, interessi, preferenze.[72]

Il tema è di stretta attualità nei settori dell'affidabilità creditizia, assicurativo, delle assunzioni elettroniche di personale, del rendimento lavorativo, nell'analisi comportamentale.

Un processo decisionale automatizzato che produca effetti giuridici o che incida significativamente sui diritti delle persone può essere, per il Regolamento europeo, accettabile se necessario per la conclusione o esecuzione di un contratto o se vi sia stato un consenso espresso dell'interessato.

Un rilievo preminente è dato, in sede di resa delle informazioni sul trattamento dei dati personali (artt. 13 e 14), alla specificazione che deve essere data all'interessato sull'esistenza di un processo decisionale automatizzato, compresa la profilazione[73].

7. LA VALUTAZIONE DI IMPATTO (CENNI)

La corretta predisposizione delle misure di sicurezza e l'esecuzione degli altri adempimenti previsti dalla normativa possono talvolta non essere sufficienti a garantire un corretto adeguamento di coloro che trattano dati personali.

In talune ipotesi, dopo avere elaborato le misure di sicurezza ritenute più adeguate al caso concreto e sviluppato una analisi del rischio, potrebbe essere necessario valutare l'impatto che il trattamento potrebbe avere nei confronti dei diritti e degli interessi fondamentali degli individui.

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il GDPR obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

---

[72] Il tema e le analisi sono molteplici: si veda, già cit. in nota 6: M. DELMASTRO – A. NICITA, Big Data. Come stanno cambiando il nostro mondo, il Mulino, 2019. Un recente contributo relativo alle questioni e ai connessi rischi dell'utilizzo di grandi quantità di dati mediante sistemi automatizzati è stato pubblicato su Il Corriere Giuridico, 12/2019: *Big Data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi*, 1517 e ss..

[73] Si veda, più compiutamente, il Manuale Europeo della Protezione dei dati, pagg. 258 e ss..

Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l´osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

L'**art. 35 del Regolamento**, soprattutto con riferimento all'utilizzo delle tecnologie più moderne, prevede una apposita procedura: in particolare, quando un trattamento, come accennato, prevedendo l'utilizzo di nuove tecnologie, considerati natura, oggetto, contesto e finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare è tenuto, prima di procedere al trattamento, a effettuare una valutazione di impatto. L'obbligo sorge, in particolare, laddove siano effettuati:

a) una valutazione sistematica e globale di aspetti personali basata su trattamenti automatizzati, compresa la profilazione e sulla quale si fondino delle decisioni;
b) il trattamento su larga scala di categorie particolari di dati personali (artt. 9 e 10 del regolamento, i cc.dd. dati "sensibili")
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Si segnala qui, per ragioni di economia, la ricca pagina informativa del Garante Privacy, con rimandi anche alle Linee Guida del Gruppo Articolo 29 e ai chiarimenti forniti[74].

8. LA VIOLAZIONE DEI DATI PERSONALI (CENNI)

Una violazione di dati personali è qualsiasi infrazione alla sicurezza dei dati personali che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Titolare o dai Responsabili[75].

La violazione dei dati personali può essere suddivisa in tre categorie:

- "**Confidentiality breach**": in caso di divulgazione o accesso non autorizzato o accidentale a dati personali;
- "**Availability breach**": in caso di alterazione non autorizzata o accidentale di dati personali;
- "**Integrity breach**": in caso di modifica non autorizzata o accidentale di dati personali.

Una violazione può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio

[74] https://www.garanteprivacy.it/regolamentoue/DPIA.
[75] Per approfondimenti, si veda PRIVACY. Protezione e trattamento dei dati. IPSOA MANUALI – WOLTERS KLUWER, 2020, pagg. 305 e ss..

perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Vale la pena evidenziare che se tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

Le Violazioni possono accadere per un ampio numero di ragioni che possono includere:

- ✔ divulgazione di dati personali a persone non autorizzate;
- ✔ perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- ✔ perdita, furto o distruzione di documenti cartacei;
- ✔ infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- ✔ accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- ✔ casi di pirateria informatica;
- ✔ banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- ✔ virus o altri attacchi al sistema informatico o alla rete aziendale;
- ✔ violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- ✔ smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- ✔ invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

Per accesso non autorizzato, che costituisce una violazione ai dati personali, si intende l'accesso di chiunque sia considerato terzo, pertanto qualsiasi soggetto che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

GLI ADEMPIMENTI PRATICI

1. LO STUDIO E GLI ENTI AMMINISTRATI

Come abbiamo visto sommariamente (e in modo incompleto rispetto alle complessive norme del GDPR) nelle pagine precedenti, il Regolamento Europeo pone in capo al Titolare del trattamento, ossia alla "persona fisica o giuridica, all'autorità pubblica, al servizio o all'organismo che singolarmente o insieme ad altri determina le finalità e i mezzi del trattamento" (art. 4, p. 1, n. 7), l'onere

- di **rispettare il Regolament**o stesso e
- di **essere "in grado di comprovarlo"** (art. 5, p. 2).

E' dunque il Titolare il soggetto cui compete il rispetto dei principi generali sommariamente enunciati sopra e l'onere di essere in grado di avere adottato misure tecniche e organizzative adeguate per rispettare i principi in tema di trattamento dei dati personali, ossia che "il trattamento è effettuato conformemente al regolamento" (art. 24, p. 1).

La normativa sul trattamento dei dati è assai importante perché **ogni Amministratore**, nell'espletamento delle proprie attività, siano esse relative ai Condomìni amministrati, siano esse relative alla gestione dello Studio professionale, "**tratta" numerosi "dati personali**".

Basti pensare, per fare un esempio, alle informazioni, e quindi ai "dati":

- necessari allo svolgimento del rapporto contrattuale di lavoro *con i propri dipendenti o collaboratori* di **Studio**,
- oppure ai *rapporti in essere con clienti e fornitori*, nel corso dei quali è fisiologico trattare dati personali come nomi e indirizzi, indirizzi di posta elettronica, di spedizione, codici fiscali, numeri di telefono e così via;

Per quanto riguarda i **Condomìni**, si pensi:

- ai dati dell'Ente complessivamente considerato come ente di gestione e, pertanto, a tutte le informazioni personali necessarie per la gestione della proprietà comune, ad esempio ai dati relativi ai consumi collettivi, ma anche ai dati e alle informazioni di eventuali dipendenti (un portiere) e fornitori;
- ai dati e alle informazioni riferite ai singoli partecipanti, i condòmini (proprietari ma anche conduttori), raccolti e utilizzati per adempiere alle obbligazioni nascenti dal rapporto di mandato e anche a quelli raccolti per le finalità riconducibili alla disciplina civilistica, come ad esempio ai dati anagrafici e gli indirizzi necessari per convocare le assemblee, o per verificare la regolare costituzione delle stesse, oppure per verificare se

siano raggiunti i quorum deliberativi necessari; si pensi a tutto quanto contenuto nell'anagrafe condominiale, come previsto dall'art. 1130 codice civile.

In Studio ma anche e soprattutto in Condominio, pertanto, luogo di stretta convivenza tra le persone, è essenziale l'equilibrio tra la trasparenza di gestione della cosa comune e il diritto alla riservatezza dei partecipanti.

IL RUOLO DELL'AMMINISTRATORE DI CONDOMINIO NELL'INTERPRETAZIONE DEL GARANTE DELLA PRIVACY

Il **Titolare del trattamento**, come già accennato, è l'ente o il soggetto che, singolarmente o insieme ad altri, "*determina le finalità e i mezzi del trattamento di dati personali*" (Art. 4, 7. del GDPR). Nello studio professionale, pertanto, tale ruolo deve essere individuato nel singolo professionista titolare, nello studio associato o nella società in concreto presente, sia essa una società di persone (s.a.s., s.n.c.) oppure una società di capitali (s.r.l., s.p.a., ecc.).

In tali enti, società di persone o di capitali, è la *persona giuridica* a essere qualificata *Titolare*, anche se, ovviamente, essa agisce, in ogni propria attività, in persona del legale rappresentante. Ne deriva che, in Studio, il professionista, l'ente, la Società o lo Studio associato, sono Titolari del trattamento dei dati dei rispettivi dipendenti, collaboratori, clienti, fornitori e così via.

Ai sensi del GDPR il **Responsabile** è, invece, colui (persona fisica o giuridica) che "*tratta i dati personali per conto del Titolare*" (Art. 4, 8. GDPR).

Nella compagine condominiale **l'amministratore di condominio deve, a parere del Garante Privacy, essere inquadrato come un Responsabile**.

Da tempo, infatti, il l'Autorità Garante individua nell'amministratore di condominio colui che "**tratta i dati per conto** del Titolare", ossia **dell'ente condominio** complessivamente considerato.

Una delle ragioni di tale impostazione, nota e condivisibile è, per esempio, che al termine del proprio mandato, ai sensi dell'Art. 1129 c. 8 del codice civile, l'amministratore deve riconsegnare tutti i "dati", ossia le carte e i documenti - oltre al denaro contante - dei condòmini e del condominio a quest'ultimo o, eventualmente e frequentemente, al nuovo amministratore.

Ciò perché, come si va esponendo, **i "proprietari" delle informazioni** (dati personali) contenute in questa documentazione **sono i singoli interessati**, mentre il Titolare del trattamento è, e rimane, il Condominio nella propria interezza di compagine e di ente di gestione.

Nelle già citate Prescrizioni del Garante del 18 maggio 2006 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1297626#) si legge infatti:

le informazioni "*... in termini generali, possono formare oggetto di trattamento da parte della compagine condominiale unitariamente considerata – di regola con l'ausilio dell'amministratore di condominio (nell'eventuale veste di responsabile del trattamento ai sensi degli artt. 4, comma 1, lett. g), e 29 del Codice* – "vecchio" codice, ndr*)...*"; e ancora:

"*per prevenire illecite comunicazioni e diffusioni di dati personali devono essere adottate, se del caso anche a cura dell'amministratore del condominio, idonee misure di sicurezza ...*";

"*ove si intenda esercitare il diritto d'accesso [...], tale facoltà compete al rappresentante della compagine condominiale, di regola l'amministratore*";

"rispetto alle informazioni personali relative al singolo partecipante, [...], resta salvo il diritto del medesimo di accedere ai dati che lo riguardano [...]. Tale diritto può essere esercitato nei confronti del condominio (inteso come la collettività dei partecipanti), anche presentando la relativa istanza all'amministratore".

Queste prescrizioni confermano che all'amministratore, nello svolgimento dell'attività e del mandato conferitogli dall'assemblea condominiale è attribuita la qualifica di Responsabile del trattamento dei dati personali per conto del Titolare – Ente Condominiale.

↓ ↓ ↓

Ciò comporta, di conseguenza, che l'amministratore debba operare una distinzione, in tema di adeguamento al GDPR, quando le operazioni di "trattamento dei dati personali" siano svolte nell'ambito della propria attività professionale rispetto a quando, invece, le operazioni vengano effettuate nella qualità di Amministratore di un singolo Condominio.

Per ciascun Condominio amministrato, dunque, **è opportuno prevedere**, sino a vigenza dell'interpretazione che stiamo esaminando, **la formalizzazione della qualifica di Responsabile del trattamento dell'Amministratore**, mediante apposita (convocata e deliberata) verbalizzazione assembleare.

2. COME PROCEDERE. GLI ADEMPIMENTI

Le norme del GDPR prevedono la gestione ed esecuzione di una serie di attività come, ad esempio:

- l'adozione, la tenuta e l'aggiornamento del c.d. ***Registro dei Trattamenti***, strumento, indispensabile per ogni realtà organizzativa (si veda l'art. 30 del Regolamento);

- la predisposizione e l'aggiornamento delle ***Informative*** ("Informazioni" all'interessato: art. 13 GDPR, ad es.) e dei ***consensi***, ove necessari; si rammenta, al riguardo, che è ancora attuale il provvedimento del Garante della Privacy in tema di amministrazione condominiale che dispone che l'Amministratore, salvo l'interessato non abbia già reso, con altre modalità, pubblici la propria utenza cellulare e il proprio account personale di posta elettronica, sia tenuto a chiedere e ottenere dal medesimo condòmino il consenso al relativo trattamento, da effettuarsi, ovviamente, nel rispetto di tutte le altre norme già indicate[76];

L'AMMINISTRATORE PUÒ UTILIZZARE I NUMERI DI TELEFONO O GLI INDIRIZZI E-MAIL DEI CONDÒMINI?

I numeri di telefono fisso, di telefono cellulare e l'indirizzo di posta elettronica possono essere utilizzati se sono già indicati in elenchi pubblici (come le pagine bianche o le pagine gialle) oppure se l'interessato abbia fornito il proprio consenso. In ogni caso, occorre sempre tenere presente il principio di proporzionalità circa l'uso di tali recapiti, con particolare riferimento a frequenze e ad orari: il loro utilizzo può essere opportuno in casi di necessità ed urgenza (soprattutto per evitare situazioni di pericolo o danni incombenti), mentre occorre massimo discernimento per le attività ordinarie e non possono essere comunicati a terzi.

6 • GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- la designazione dei collaboratori di Studio quali ***autorizzati al trattamento***; per quanto riguarda gli Enti amministrati, verificare la presenza del portiere, del custode o di altri soggetti che debbano essere correttamente autorizzati al trattamento e, anche, come precisato nel punto seguente, specificamente istruiti in tal senso;

- la formazione e la predisposizione, per gli incaricati, di specifiche ***istruzioni*** sul trattamento dei dati personali, oltre che alla previsione di un'aggiornamento di tale formazione;

[76] Si veda al link:https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2680257.

ad esempio chi elabora le buste paga), con adeguata **contrattualizzazione** di questi rapporti; per quanto riguarda gli Enti amministrati, è evidente come possano ricorrere, in molti casi, ipotesi in cui sia il Condominio a esternalizzare alcuni servizi: in tali casi è opportuna una attenta disamina delle ipotesi e, in ogni caso, una contrattualizzazione volta ad assicurare sicurezza e protezione dei dati sia condominiali sia dei partecipanti, da parte del fornitore (si pensi alle imprese di pulizia, alle imprese che effettuano lavori in condominio, ai fornitori, ai manutentori, alle imprese specializzate che accedono per i lavori e le prestazioni più disparate: esse hanno accesso, in taluni casi, alle informazioni, sia dell'ente complessivamente considerato sia dei singoli partecipanti);

- l'individuazione di coloro che si occupano dei sistemi elettronici con funzione di ***amministratori di sistema*** (come le società o i professionisti che si occupano della gestione e manutenzione del software di studio), con i quali devono essere stipulati **precisi accordi** in materia di gestione e tutela dei dati personali;

- l'individuazione e predisposizione di adeguate ***misure di sicurezza*** per la protezione dei dati personali, intese come misure *fisiche* (come ad esempio le porte blindate, l'antifurto, gli schedari opportunamente dotati di chiavi per l'accesso, ecc.), *logiche e tecnologiche* (come l'adozione di software antivirus, antispam, di protezione contro i malware, l'esecuzione di periodici back up, ecc.) e *organizzative* in senso generale.

- Non per ultimo, le norme prevedono l'adozione di altre procedure in tema, ad esempio, di **riscontro alle richieste degli interessati** nonché

- in tema di possibili **incidenti di sicurezza**, come potrebbero essere quelli causati dalla perdita di informazioni, dall'accesso non autorizzato ad esse, ecc..

- Un tema, infine, di estrema importanza, è rivestito dalla **Videosorveglianza**, sia se predisposta nello Studio sia se adottata dall'assemblea Condominiale. L'argomento e la disciplina sono complesse e delicate, trattandosi, senza dubbio, di trattamento di dati personali. Precisato che l'Ente Europeo per la protezione dei dati ha recentemente pubblicato delle Linee Guida di cui si attende una "versione" della nostra Autorità, si rimanda, per ragioni di spazio, ai seguenti link: https://www.garanteprivacy.it/documents/10160/10704/Provvedimento+in+materia+di+videosorveglianza+-+leaflet+.pdf/6c3df7ec-7f25-4d5f-9ef9-eaebf6e9f0df?version=1.2; https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1002987.

Come ben si vede le attività e le procedure sono tante e diversificate: è necessario che tutto quanto il Titolare compie per adeguare la propria realtà lavorativa sia, se richiesto, **documentabile**.

3. L'AGGIORNAMENTO E IL MANTENIMENTO

Come più volte accennato, la protezione dei dati personali è divenuta un obiettivo da tenere costantemente presente in pressoché tutte le realtà commerciali, produttive e consulenziali.

La corretta adozione di misure tecniche e organizzative che consentano di "proteggere" realmente le informazioni di cui le aziende dispongono e che utilizzano è imprescindibile nella odierna realtà "*data driven*"[77].

Sarà dunque necessario progettare, prevedere, organizzare un costante mantenimento e aggiornamento delle procedure e dei processi sviluppati, con verifiche periodiche sia delle stesse procedure sia delle misure adottate, unitamente alla ulteriore verifica della loro adeguatezza con riferimento al caso concreto.

Gli esperti suggeriscono dunque di prevedere, mediante costante e continua assistenza e consulenza, sia da un punto di vista strettamente privacy sia da un punto di vista prettamente tecnologico, le seguenti ulteriori attività:

- Aggiornamenti annuali della complessiva "compliance";
- Aggiornamenti periodici delle misure tecniche It e delle procedure *by design* e *by default*;
- Aggiornamenti a adattamenti, se necessari, dei registri delle attività di trattamento;
- Consulenza e assistenza nell'adozione di eventuali *tool* di verifica dell'*assessment*;
- Per tutto ciò che può concernere il modo tech (Advertising tecnology, web services, piattaforme, e-commerce, internet of things, domotica, trasferimenti extra Ue, sanità, ecc.) la consulenza e l'assistenza in materia di data protection sono imprescindibili[78];
- Infine, ma non per ultimo, il settore dei servizi di Data Protection Officer, Responsabile della Protezione dei dati è in costante, necessario aumento.

---

[77] Un recente studio conferma che il 70% delle aziende che ha sviluppato procedure in tema di data protection ha ottenuto benefici notevoli: https://www.corrierecomunicazioni.it/privacy/data-protection-leva-di-business/.

[78] Si vedano le recentissime sanzioni dell'Autorità Garante a Tim: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256409 e a Eni Gas e Luce: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9244351.