Rapporti tra Condominio - Amministratore - Fornitori di servizi alla luce del GDPR. Problemi applicativi, conseguenze, possibili soluzioni

Occorre ricordare quali siano i rapporti, alla luce del c.d. "GDPR" (più esattamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], Regolamento U.E. n.679/2016 sul trattamento dei dati personali), tra Condominio, Amministratore del Condominio ed eventuali ulteriori soggetti che forniscano servizi al Condominio, in particolare se parliamo di servizi informatici e/o telematici.

Il funzionamento del Condominio è regolato dagli articoli del Codice civile, con i quali devono necessariamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], essere messi in relazione logica le regole derivanti dal GDPR.

Prima di passare ad analizzare le impostazioni generali, che dovrebbero essere esistenti PRIMA che la messa in opera di tutti i servizi relativi alle assemblee on line siano decisi, come ampiamente trattato dagli altri coautori, occorre ragionare sulle possibili conseguenze della mancata adozione di quello che verrà descritto, in maniera abbastanza sintetica, nel prosieguo.

Il ragionamento fondamentale che l'Amministratore di Condominio, quale soggetto professionista [salvo i rari casi di amministrazione affidata da un condòmini] ha le medesime responsabilità previste dal codice civile per i professionisti esercenti le c.d. "professioni ordinistiche" [medici, avvocati, ingegneri, architetti, ecc. ecc.], conseguentemente risponde del proprio operato dovendo dimostrare di aver svolto il proprio lavoro non solamente con la diligenza del *buon padre di famiglia*, ma con la diligenza correlata alla professione esercitata e quindi, di conseguenza, risponde anche per la c.d. *colpa lieve*, locuzione che vuol dire che si deve dimostrare che il compito svolto aveva in sé particolari difficoltà, per non incorrere

in responsabilità. L'esempio generalmente utilizzato è quello della responsabilità medica per una operazione di routine (asportazione appendice), che *in pratica* non è più ammissibile alla luce dei progressi della diagnostica, e per una operazione comunque ad alto rischio (asportazione di formazione neoplastica situata in particolari zone del cervello).

Applicando questi semplici principi alla c.d. *videoassemblea*, si deve conseguentemente pensare a quali potrebbero essere le conseguenze della mancata *previa* applicazione di quanto infra verrà precisato.

Limitandosi solamente ad alcuni problemi fondamentali:

I. Possibilità di essere esposti ad azioni di risarcimento ai sensi del GDPR per trattamento illecito di dati personali (responsabilità di tipo civilistico)
II. Possibilità di essere esposti a sanzioni da parte dell'Autorità Garante del trattamento dei dati personali (responsabilità di tipo pubblicistico)
III. Possibilità di essere esposti a sanzioni di tipo penale ai sensi del GDPR per trattamento illecito di dati personali (responsabilità di tipo penalistico)
IV. Possibilità di nullità, quanto meno parziale, dei contratti stipulati, per nullità, quanto meno parziale, **dell'oggetto del contratto**, *per il mancato rispetto di norme imperative*, come sono quelle imposta dal G.D.P.R.

Le definizioni specifiche concernenti il GDPR sono descritte più avanti, quello che occorre comprendere che TITOLARE ai sensi del GDPR è il condominio nella sua interezza, il quale manifesta la propria volontà attraverso l'assemblea condominiale.

Il CONDOMINIO-TITOLARE nomina l'Amministratore, che dal punto di vista del Codice Civile è l'ORGANO di rappresentanza del Condominio-Titolare, ma NON È il titolare. A sua volta se l'amministratore è costituito giuridicamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], in forma diversa dalla ditta individuale, l'Amministratore-RESPONSABILE

(primario) sarà il soggetto giuridico diverso dalla ditta individuale, il quale avrà a propria volta un legale rappresentante, che è l'organo di rappresentanza di tale soggetto giuridico. Per fare un paragone occorre pensare all'amministratore unico di una S.r.l. ed alla società stessa; Titolare è la società, l'A.U. è l'organo che agisce per conto della società.

Conseguentemente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], quando l'Amministratore (in qualunque forma giuridica sia costituito) agisce in nome e per conto del condominio, va fatto riferimento alle norme del codice civile, **mentre** quando l'Amministratore-RESPONSABILE (primario) (in qualunque forma giuridica sia costituito) tratta nel proprio ufficio i dati derivanti dal rapporto con il Condominio-Titolare, si deve fare riferimento alla normativa in materia di "privacy".

Da ultimo, occorre precisare che il Condominio-Titolare attraverso l'approvazione di determinati documenti deve fornire delle istruzioni all'Amministratore-Responsabile, ma ovviamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], non può ingerirsi direttamente nella organizzazione lavorativa dell'Amministratore-Responsabile, in quanto trattasi di soggetto giuridicamente distinto, a meno che tali scelte (sub responsabili) non concernano il rapporto Titolare-Responsabile, quindi il Condominio dovrà dotarsi di linee guida con l'annesso regolamento che l'Amministratore-Responsabile dovrà adottare per la violazione delle Linee Guida, che consentano di affrontare in maniera organica gli obblighi normativi in materia di protezione dei dati personali, così da conseguire i migliori risultati nel proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dalla normativa comunitaria e nazionale

Tali documenti sono necessari per definire il Modello Organizzativo Privacy, ovvero individuare strategia, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dal Titolare [Condominio] attraverso l'Amministratore

[Responsabile Primario/Principale], anche attraverso il riferimento ad un sistema di documenti esterni ma richiamati, atti a formare un corpo unico di norme per il Condominio-Titolare ma soprattutto per l'Amministratore-Responsabile, ai sensi del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (Codice della Privacy), come modificato dal D.Lgs. 10 agosto 2018, n. 101 e del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (GDPR – General Data Protection Regulation), nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione delle *policy (regole)* da parte del Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale].

In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del "Codice della Privacy" e del "GDPR", anche con riferimento alle decisioni e ai provvedimenti emessi dal Garante Europeo della Protezione dei Dati (GEPD) e dall'Autorità Garante Nazionale per la protezione dei dati personali.

Ai fini del Modello Organizzativo Privacy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

1. Regolamento: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati);
2. Normativa: D.Lgs. 2003/196 (come modificato dal D.Lgs. 2018/101) e Regolamento (UE) 2016/679, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione da parte del Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], Modello Organizzativo Privacy.

3. Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
4. Soggetti esterni: soggetti giuridici giuridicamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], al condominio da vari tipi di rapporti giuridici, con esclusione del rapporto di lavoro subordinato e rapporti ad esso assimilabili, che potrebbero essere stabilite nel territorio dello Stato italiano o in un luogo comunque soggetto alla sovranità dello Stato italiano,
5. Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], o indirettamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
6. Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
7. Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
8. Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

9. Interessato: la persona fisica cui si riferiscono i dati personali;
10. Soggetto Autorizzato: tutte le persone, sia che ricoprano delle funzioni dirigenziali o apicali, sia che lavorino semplicemente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], come lavoratori subordinati o del Condominio-Titolare o dell'Amministratore-Responsabile, ivi compresi i legali rappresentanti di tali due soggetti, sono sempre persone autorizzate al trattamento, che ovviamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], avranno profili diversi di accesso ai dati in funzione della specifica mansione espletata.
11. Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
12. Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
13. Referente: il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], per la protezione dei dati personali (DPM - Data Protection Manager): la persona fisica preposta alla sorveglianza sull'applicazione e il rispetto delle disposizioni in materia di trattamento di dati impartite dal Titolare del trattamento e, per quanto di sua competenza se nominato da quest'ultimo, dal DPO;
14. Referente privacy: il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile con compiti di coordinamento di più o soggetti autorizzati (o designati);
15. Incaricato: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento (anche soggetti designati);

16. Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate [incaricati] al trattamento dei dati personali sotto l'autorità diretta del titolare del trattamento o del responsabile del trattamento;
17. Asset pertinenti al Condominio, le varie articolazioni nelle quali può essere diviso il trattamento dei dati riferiti al Condominio.
18. Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
19. Trattamento transfrontaliero: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], inciderebbe in modo sostanziale sugli interessati in più di uno Stato membro.
20. Paesi terzi: paesi non appartenenti all'UE o allo spazio Economico Europeo (Norvegia, Islanda, Liechtenstein)

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure interne alla struttura dell'Amministratore-Responsabile, rispetto alle quali il Titolare [Condominio] attraverso l'Amministratore [Responsabile

Primario/Principale], pretende l'integrità e la protezione e conseguentemente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], l'accesso esclusivamente da parte del Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], ai ruoli e alle funzioni necessarie e preventivamente autorizzate da parte del Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale],

La mancanza di adeguati livelli di sicurezza può infatti comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione della Clientela il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], il rischio di incorrere in sanzioni legate alla violazione delle leggi vigenti nonché altri danni di natura economica e finanziaria.

Per conseguire sempre l'allineamento normativo e aumentare la capacità di controllo l'mente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], ha – come per legge e sempre attraverso l'Amministratore-Responsabile - istituito e mantiene aggiornato un registro delle attività di trattamento.

Il condominio identifica, quando ritenuto necessario a seguito delle risultanze dell'analisi dei rischi connessi al trattamento dei dati personali, le ulteriori esigenze di sicurezza tramite la valutazione di impatto sulla protezione dei dati che conseguentemente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], di acquisire un livello aggiuntivo di consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati.

La valutazione del rischio, eseguita su tutti i trattamenti in essere o previsti, permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione delle misure di sicurezza al sistema informativo e in generale all'intera organizzazione, oltre a indicare quale sia la probabilità che le minacce identificate trovino reale attuazione. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

La gestione della sicurezza delle informazioni è fondata su alcuni imprescindibili principi generali, di seguito enunciati:

1. Esiste un catalogo costantemente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], aggiornato degli asset pertinenti al Condominio, rilevanti ai fini della gestione delle informazioni e per ciascuno di essi è individuato un responsabile;
2. Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti e appropriati;
3. Gli accessi ai sistemi informativi sono sottoposti a una procedura di identificazione e autenticazione. Inoltre, le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti dai singoli individui, in modo che ogni utente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], possa accedere alle sole informazioni di cui necessita, e tali autorizzazioni sono periodicamente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], sottoposte a revisione (come previsto dal Regolamento Informatico);
4. Sono definite delle procedure per l'utilizzo sicuro dei beni (luoghi, mezzi di trasporto, strumenti) e delle informazioni pertinenti al Condominio,
5. È incoraggiata la piena consapevolezza da parte del personale delle problematiche relative alla sicurezza delle informazioni;
6. Per poter prevenire o almeno gestire in modo tempestivo gli incidenti, tutti sono chiamati a rendersi partecipi del sistema di sicurezza aziendale e pertanto devono notificare qualsiasi problema relativo alla sicurezza di cui sono a conoscenza;
7. È necessario prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni;
8. È assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;

9. È predisposto un piano di continuità che permette all'azienda di affrontare efficacemente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale. Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici;
10. Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

MONITORAGGIO DEL SISTEMA GESTIONE PRIVACY

Il Responsabile (Amministratore) verifica almeno una volta all'anno l'efficacia e l'efficienza del Sistema di Gestione della Privacy, in modo di assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo.

La revisione deve verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica privacy delle procedure in atto così come di quelle previste e non ancora applicate.

Deve inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato dell'intero processo di revisione periodica include tutte le decisioni prese e le azioni adottate in merito al miglioramento del Sistema di Gestione della Privacy.

INFORMAZIONE E FORMAZIONE

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dall'mente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], anche e soprattutto grazie alla particolare attenzione risposta nei confronti della formazione del proprio personale.

A tale scopo il Modello Organizzativo Privacy è divulgato presso il personale già in servizio e, nel caso di nuove risorse umane inserite in organico, fin dal momento del loro ingresso nella compagine dell'mente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale].

Per gli stessi fini di conoscenza eventuali aggiornamenti sono diffusi con gli strumenti ritenuti di volta in volta più efficaci.

Allo scopo creare un ecosistema favorevole nell'ambiente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], di lavoro e formare con particolare cura i soggetti che per il ruolo ricoperto risultano inseriti nel Sistema di Gestione della Privacy, l'mente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale]:

1. adotta un piano formativo con l'obiettivo di alfabetizzazione iniziale in materia di protezione dei dati personali, destinato a tutto il personale della società;
2. prevede l'erogazione di moduli specifici all'interno dei corsi di formazione per il ruolo ricoperto, sia in quelli organizzati all'immissione in servizio che al momento del cambio di mansione qualora sia di livello superiore o per ambito applicativo diverso;
3. prevede un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito privacy a tutti i dipendenti della società;
4. conserva la documentazione distribuita e la modulistica attestante la partecipazione agli interventi formativi.

5. La formazione dei soggetti autorizzati al trattamento e, ove ritenuto necessario, delle altre figure chiave nel Sistema di Gestione della Privacy, riguarda in particolare:
6. gli aspetti generali della disciplina di protezione dei dati personali;
7. le minacce, le vulnerabilità, la probabilità di accadimento e di conseguenza i rischi che minacciano i dati trattati;
8. le conseguenze derivanti dalla violazione dei dati personali (Data Breach);
9. le procedure da seguire in caso di violazione dei dati personali;
10. le misure di prevenzione per evitare o almeno ridurre la probabilità di accadimento delle violazioni e le misure di mitigazione del danno in caso si verifichino;
11. gli aspetti specifici della disciplina di protezione dei dati personali nel settore di azione dell'mente il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], (con particolare attenzione per gli ambiti sanitario, TELCO, bancario, ecc.);
12. l'addestramento specifico per aggiornare il personale sulle misure di sicurezza e protezione dei dati personali ritenute adeguate e adottate dal Titolare del trattamento.

La formazione deve essere:

1. adeguata al proprio sistema di trattamento dei dati personali;
2. efficace nella trasmissione delle informazioni in materia di protezione dei dati personali;
3. il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], nel fornire strumenti per l'esecuzione delle procedure previste dal Sistema di Gestione della Privacy;
4. documentabile, ovvero erogata da soggetto che possa certificare l'avvenuta formazione e l'avvenuto superamento di un livello minimo di comprensione, in quanto la formazione è parte integrante della policy con la quale il Titolare [Condominio] attraverso l'Amministratore [Responsabile Primario/Principale], e

l'articolazione e gli esiti di tale attività devono essere sempre disponibili.

Soggetti autorizzati al trattamento

il Responsabile del Trattamento nomina, presso le Unità Organizzative in cui vengono svolti i trattamenti, i soggetti autorizzati al trattamento dei dati (o soggetto designato o INCARICATO).

L'incaricato effettua tutte le operazioni di trattamento dei dati personali attinenti all'attività lavorativa di competenza dell'area di appartenenza e opera sotto l'autorità del Titolare (o del Responsabile del Trattamento), attenendosi alle istruzioni dallo stesso impartite nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui lo stesso abbia accesso.

In particolare, i compiti a esso attribuiti sono così sintetizzati:

1. segnalare al Responsabile privacy da cui dipende, o al Data Protection Officer – DPO nel caso di dipendenza diretta, eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
2. avvisare il Responsabile privacy da cui dipende, o il Data Protection Officer – DPO nel caso di dipendenza diretta, se nello svolgimento di un'attività dovesse riscontrare il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il registro dei trattamenti ed eseguire almeno un'analisi dei rischi, in applicazione dei principi di privacy by design e privacy by default;
3. informare immediatamente il Responsabile privacy da cui dipende, o il Data Protection Officer – DPO nel caso di dipendenza diretta, qualora le istruzioni ricevute risultino non conformi alla normativa sulla protezione dai dati;
4. segnalare al Responsabile privacy da cui dipende, o il Data Protection Officer – DPO nel caso di dipendenza diretta, eventuali accessi non autorizzati;

5. rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare del trattamento (o del Responsabile del trattamento di riferimento).

Amministratore di Sistema

La figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi (system administrator), ovvero una base dati (database administrator), ovvero reti e apparati di telecomunicazione di sicurezza (network administrator) è nominata persona autorizzata al trattamento dei dati personali con la qualifica specialistica di Amministratore di Sistema.

L'attribuzione delle funzioni di Amministratore di Sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza.

La nomina ad Amministratore di Sistema deve essere individuale, esplicitata in forma scritta, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.

In generale, l'Amministratore di sistema ha le seguenti responsabilità:

1. sovraintendere alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;
2. in accordo con il Data Protection Officer – DPO, fornire guida e supporto ai Referenti Privacy e ai soggetti autorizzati in merito al trattamento dei dati personali;
3. amministrare e gestire la sicurezza informatica operando anche come gestore e custode delle password;
4. nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche, in merito a quanto previsto dal

Regolamento Informatico del Sistema di Gestione della Privacy (SGP);

5. individuare i soggetti a cui affidare l'incarico di manutentore del sistema stesso.

L'amministratore di Sistema che provvede alla designazione dei soggetti incaricati alla manutenzione deve preventivamente informare il Responsabile del Trattamento e deve formalizzare per iscritto l'attribuzione dell'incarico eventualmente specificando i limiti dell'intervento e le manutenzioni richieste.

Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali avarie hardware, ma anche gli interventi volti alla ricostruzione di archivi che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato.

Per consentire all'Amministratore di Sistema di svolgere adeguatamente le proprie funzioni, allo stesso vengono concesse dal Titolare del trattamento le "Autorità di sistema", che consistono nell'assegnazione di attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati.

Tornando al discorso delle conseguenze del mancato rispetto delle regole imposte dal G.D.P.R., in effetti – purtroppo – non vi è una soluzione facile, se non quella di adeguarsi e di affidarsi a professionisti seri e con adeguato c.v.
L'alternativa è quella di affidarsi alla c.d. *buona sorte.* ☺

Avv. Luca-M. de Grazia