

Azienda Agricola Merra Pierluigi

VIA BISCEGLIE, 46 - CAP 76123 - ANDRIA(BT)

15/11/2021

REGOLAMENTO UE 679/2016

GAP ANALYSIS

Tipologia di dati personali trattati

- **Dati identificativi:** nome e cognome, codice fiscale, data e luogo di nascita, dati relativi all'ubicazione, documento di riconoscimento/patente/passaporto, indirizzi e-mail, numeri telefonici, coordinate bancarie ed elementi caratteristici dell'identità economica, immagini.
- **Categorie particolari di dati personali definiti anche "sensibili":** dati idonei a rilevare lo stato di salute.

Categorie di soggetti sottoposti al trattamento dei dati personali

- Candidati all'assunzione
- Clienti
- Fornitori
- Dipendenti e propri familiari
- Altro (agenti)

Flusso dati interno

L'analisi condotta ha evidenziato all'interno dell'organizzazione aziendale un costante flusso di dati relativo a persone fisiche, trattati per differenti scopi e finalità.

L'azienda raccoglie e gestisce:

1) i **dati del Personale dipendente** per eseguire il contratto di lavoro o per ottemperare a specifici obblighi di legge. Ai dipendenti sono richiesti **dati identificativi** e **particolari categorie di dati (ex dati sensibili).**

   Tra i dati ex sensibili raccolti vi sono i dati relativi allo stato di salute (certificati medici per malattia e infortunio).

   I dati relativi al personale, sensibili e identificativi, sono trattati unicamente all'interno dell'ufficio amministrativo dai soggetti incaricati alla gestione delle pratiche dei dipendenti.

2) i **dati personali dei fornitori** per usufruire dei servizi di manutenzione, consulenza, trasporto e per l'acquisto dei beni funzionali allo svolgimento dell'attività principale. A queste categorie di soggetti sono richiesti unicamente i **dati identificativi** per predisporre l'ordine di acquisto e provvedere all'esecuzione della fornitura. Suddetti dati sono trattati all'interno dell'ufficio amministrativo dal personale incaricato agli acquisti.

3) i **dati personali dei clienti** per gestire le relazioni commerciali e provvedere alla consegna del prodotto finale. A queste categorie di soggetti sono richiesti i dati identificativi al fine di predisporre l'ordine di vendita, per eseguire la commessa, per procedere alla fatturazione e per alimentare o tutelare il rapporto commerciale. Suddetti dati sono trattati all'interno dell'ufficio amministrativo.

4) i **dati personali identificativi dei candidati all'assunzione** tramite curriculum consegnato manualmente e/o tramite e-mail. Tali dati sono trattati all'interno dell'ufficio amministrativo dal personale incaricato alla gestione delle pratiche dei dipendenti.

Flusso dati esterno

I dati personali gestiti all'interno della struttura aziendale, vengono dall'azienda comunicati ai seguenti soggetti esterni:

- Istituti bancari
- Studio medico in adempimento degli obblighi in materia di igiene e sicurezza sul lavoro
- Soggetti che erogano attività professionali (consulente del lavoro, studio commerciale)
- Fornitori di servizi funzionali allo svolgimento dell'attività (vettori, manutenzione software/hardware)

PREMESSA

A seguito dell'analisi condotta mediante intervista del personale di questa società, si rappresentano, all'interno della presente relazione, gli scostamenti apprezzabili rispetto alla normativa privacy e le misure da attuare per conformarsi sia al nuovo Regolamento Europeo n. 679/2016 sia alle norme nazionali di settore in materia di protezione dei dati personali attualmente in vigore. In via preliminare, è bene sottolineare il cambio di approccio posto in essere dal GDPR (General Data Protection Regulation) rispetto al precedente Codice della Privacy (Dlgs. 30/06/2013 n. 196) in materia di misure di sicurezza da attuare per la protezione dei dati. Difatti, mentre la vecchia disciplina prevedeva un elenco dettagliato e uguale per tutti di obblighi e misure minime di sicurezza da adottare, il Regolamento introduce il principio di ***accountability*** (**responsabilizzazione**) con cui, sostanzialmente, viene affidato ai titolari il compito di decidere liberamente le modalità, le garanzie e i limiti del trattamento dei dati personali in funzione della propria attività e dei rischi ad essa connessi (Cfr. art. 24 GDPR).

Ai Titolari del trattamento non sarà più richiesto di rispettare semplicisticamente le norme, e quindi di fare una check-list di adempimenti da svolgere, ma di tradurre in pratica i principi del Regolamento attraverso una distribuzione di responsabilità all'interno dell'azienda, di adottare una strategia efficace nei confronti dei soggetti cui si riferiscono le informazioni trattate e di attuare una preventiva politica di valutazione dei rischi e delle possibili conseguenze.

In sostanza, la logica dell'*accountability* presuppone che il titolare del trattamento debba essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative e tecniche per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi. **Chi non predispone misure preventive (approccio proattivo) per garantire la corretta gestione dei dati che raccoglie è punibile per il semplice fatto di non aver garantito sicurezza alle attività di trattamento, a prescindere dall'abusivo utilizzo dei dati che ne possa essere derivato**.

Non sarà più, quindi, una materia delegabile al professionista di turno o all'esperto di tecnologia, bensì sarà l'approccio *corporate* dell'azienda ad essere valutato nella sua globalità, per tale ragione sarà essenziale documentare le scelte effettuate in termini di gestione dei dati come un vero e proprio obbligo di rendicontazione.

Sulla scorta di ciò, la protezione dei dati personali deve avvenire attraverso un metodo che segua i moderni concetti di ***privacy by design*** e ***privacy by default*** (Cfr. art. 25 GDPR).

Con la *Privacy by design* si incorpora la protezione dei dati fin dalla pianificazione del processo aziendale e della raccolta delle informazioni. Diventa obbligatorio prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati stessi. Perciò, bisognerà analizzare i flussi di dati connessi all'attività che si vuole effettuare e adottare criteri che minimizzano i rischi del trattamento e riducano le quantità di dati trattati (minimization of data).

Privacy by default, invece, significa mettere in atto meccanismi per garantire che siano trattati solo i dati necessari per ciascuna finalità specifica del trattamento, evitando di acquisire informazioni eccedenti rispetto agli obiettivi dichiarati. Con questo, la privacy diventa presupposto delle attività di trattamento e cessa di essere un obiettivo secondario da perseguire rispettando meri adempimenti formali.

In definitiva, la ratio di tali principi è responsabilizzare il soggetto titolare al fine di instaurare, autonomamente, politiche adeguate al trattamento dei dati personali in considerazione delle proprie esigenze e dei principi cardine del Regolamento stesso.

In ultimo, è opportuno precisare che tutte le prescrizioni e i principi del Regolamento si applicano esclusivamente ai "**dati personali" ossia qualsiasi informazione riguardante una persona fisica identificata o identificabile**, con esclusione, quindi, di tutti i dati riferiti a persone giuridiche (Cfr. art. 4 del Regolamento). Secondo un'interpretazione dottrinale, rientrano nel campo di applicazione del GDPR, inoltre, anche i dati riferiti a ditte individuali, liberi professionisti e società di persone in quanto, in tali situazioni, vi è una diretta coincidenza tra il soggetto giuridico e il titolare-persona fisica. Tuttavia, in mancanza di riferimenti normativi chiari e precisi in materia, sono auspicabili interventi chiarificatori da parte del legislatore e del Garante.

1. DOVERE DI INFORMAZIONE E RACCOLTA DEL CONSENSO

Il principio di trasparenza nell'ottica del GDPR impone che nessun titolare può raccogliere e trattare dati personali senza aver offerto all'interessato un'adeguata informativa che fornisca congrue delucidazioni circa il trattamento posto in essere.

A tal fine, come indicato nelle Linee guida del Gruppo art. 29 (Cfr. WP 260), è opportuno prestare attenzione affinché gli elementi da rendere noti all'interessato siano ben distinguibili rispetto ad altre informazioni, ad esempio evitando di inserire l'informativa all'interno di un testo contrattuale ma riportandola in separato allegato o ponendola comunque in evidenza.

L'informativa è una comunicazione rivolta all'interessato, cioè al soggetto al quale si richiedono i dati, finalizzata a fornire tutte le informazioni inerenti il trattamento dei dati personali. Tale adempimento, di norma, è eseguito attraverso la presentazione di un documento cartaceo da esibire insieme ad un modello di consenso, quando necessario, **prima di effettuare la raccolta dei dati personali** (art. 13 GDPR). Nel caso in cui i dati non siano raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che **non può superare 1 mese** dalla raccolta (art. 14 GDPR).

Il Regolamento prevede, altresì, che l'informativa possa essere fornita con altri mezzi, anche elettronici, o oralmente purché sia comprovata l'identità dell'interessato (Cfr art. 12 GDPR).

Tuttavia, è essenziale che tutte le informazioni di cui agli articoli in questione devono essere fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso in cui i destinatari siano minori.

Occorre, quindi, che le informazioni siano facilmente comprensibili dai destinatari, magari modulando il linguaggio in considerazione del livello di comprensione ed evitando una terminologia eccessivamente tecnica con formule astratte ed indeterminate che lasciano spazio a dubbi.

In tale prospettiva, per esempio, si inserisce l'indicazione contenuta nell'art. 12, comma 7, del GDPR secondo cui le informazioni possono essere fornite in combinazione con icone standardizzate.

Si tratta di icone che saranno definite dalla Commissione europea e dovranno essere identiche in tutta l'UE.

L' AZIENDA AGRICOLA MERRA PIERLUIGI è munita di un'informativa privacy cartacea generica, ai sensi dell'oramai abrogato art. 13 del D.lgs 196/ 2003 (Codice in materia di protezione dei dati personali), che viene presentata indistintamente ai dipendenti, fornitori e ai clienti. Tale pratica informativa, nel tempo, è stata espletata costantemente verso i soggetti soprarichiamati al momento della predisposizione delle pratiche inerenti all'assunzione (dipendenti) o durante l'instaurazione di qualunque tipo di rapporto contrattuale (clienti- fornitori).

Ciò posto, a seguito delle modifiche introdotte dal Regolamento europeo n. 679/2016 e dal decreto legislativo n.101 del 10 agosto 2018 che ha modificato parzialmente il precedente D.lgs n.196/2003, **la società in questione dovrà aggiornare e/o predisporre nuove informative privacy** con l'indicazione di tutti gli elementi tassativamente stabiliti dagli artt. 13 par. 1 e 14 par. 1 dal GDPR.

Nello specifico, dovranno essere precisati e indicati:

- I dati di contatto del titolare del trattamento e, se nominati, i dati del responsabile del trattamento e del responsabile della protezione dati (DPO);
- la base giuridica del trattamento e le finalità;
- i destinatari o le categorie di destinatari dei dati personali ed in particolare se il titolare ha intenzione di trasferire i dati in paesi extra UE;
- il periodo di conservazione dei dati e i criteri utilizzati per determinarlo;
- l'esistenza, in capo all'interessato, di una serie di diritti che dovrebbero permettergli di controllare e gestire consapevolmente il flusso dei propri dati;
- il diritto dell'interessato di presentare un reclamo all'autorità di controllo.

Particolare attenzione deve essere posta nell'individuazione del **tempo di conservazione dei dati** raccolti. Difatti, per ogni tipologia di dato raccolto, si deve specificare il periodo di custodia che non potrà essere superiore a quello necessario per il perseguimento delle finalità per cui sono stati raccolti e trattati i dati personali. A titolo esemplificativo, si pensi ai dati personali dei dipendenti o dei fornitori che dovranno essere conservati per il tempo strettamente necessario all' esecuzione di un contratto di lavoro o di fornitura oppure per adempiere a specifici obblighi previsti da norme di legge. È necessario, perciò, predeterminare una durata per ogni tipologia e categoria di dati raccolti in base alle proprie esigenze organizzative, alle attività svolte, ai propri interessi, agli obblighi di legge (es. art. 2220 c.c., art. 22 DPR 600/739) e alle specifiche dinamiche interne, indicando i criteri seguiti per stabilire tale periodo di conservazione.

2. PERSONALE DIPENDENTE E AUTORIZZATO AL TRATTAMENTO DATI PERSONALI

In materia di protezione di dati personali, il personale dipendente che tratta i dati per conto dell'azienda può assumere la qualifica di **incaricato (oggi definito autorizzato al trattamento)** con apposite nomine interne, viceversa non è più prevista la figura del **responsabile interno** del trattamento.

Dall'esame della documentazione fornita e dalle informazioni raccolte, **non è emersa una puntuale divisone dei compiti del personale della AZIENDA AGRICOLA MERRA PIERLUIGI in materia di trattamento dei dati personali attraverso la designazione con apposite lettere d'incarico ai sensi del D.lgs 196/2003.**

L'**incaricato o l'autorizzato al trattamento** è la persona fisica legittimata dal titolare a compiere operazioni di trattamento dei dati, quindi è colui che effettua materialmente le operazioni sui dati personali sotto la diretta autorità del predetto.

È importante sottolineare che, anche se tale figura non è espressamente prevista dal GDPR (art. 29 e art. 4 n. 10) come figura giuridicamente autonoma, il Garante della privacy, nella guida all'applicazione del Regolamento, giustifica e considera non incompatibile con lo stesso la figura dell'incaricato. Anzi, per il Garante, alla luce del principio di responsabilizzazione, l'uso di incaricati del trattamento (ora definite dal GDPR *persone autorizzate al trattamento)*, può essere uno strumento di *compliance* efficace per garantire proattivamente l'osservanza del regolamento nella sua interezza.

A differenza di quanto previsto nella previgente normativa, però, non si rinviene nel GDPR un obbligo di designazione formale e per iscritto degli incaricati. Tuttavia, **la designazione per iscritto è sicuramente una modalità idonea a dimostrare che il personale dipendente ha ricevuto tutte le indicazioni e istruzioni necessarie per svolgere le attività.** Difatti, è bene specificare, che la predisposizione di nomine interne deve considerarsi solo una procedura per trasmettere informazioni e focalizzare l'attenzione del personale sull'importanza di proteggere i dati personali oggetto di trattamento. Lo stesso obiettivo, a titolo esemplificativo, può essere raggiunto con altri strumenti: la pubblicazione di una politica sulla protezione dei dati personali, un regolamento interno, un disciplinare che fornisce istruzioni e assegna compiti alle funzioni organizzative.

Pertanto, **si consiglia di nominare "incaricati (autorizzato) del trattamento", tutti i dipendenti che trattano i dati personali per conto del titolare, attraverso una semplice lettera di designazione all'incarico** che contenga tutte le specifiche istruzioni di come sviluppare le attività a contatto con dati personali.

Il responsabile interno del trattamento, viceversa, si configurava come una figura interna all'azienda stessa, tecnicamente qualificata, con professionalità e conoscenze più elevate dell'incaricato, che trattava i dati per conto del titolare e doveva assisterlo nelle attività di ispezione e revisione in materia di protezione dei dati. La sua nomina era prevista dall' art. 29 dal vecchio Codice della privacy mentre non viene espressamente disciplinata dall'art. 28 del Regolamento che fa riferimento, invece, esclusivamente alla figura del responsabile esterno (Cfr. parere 1/2010 WP29), ossia una figura relativa ai soli soggetti esteriori l'azienda a cui il titolare delega alcune attività.

In considerazione di quanto suesposto, della discrezionalità di tale nomina e soprattutto del recente decreto di armonizzazione della normativa nazionale alle disposizioni del Regolamento (decreto n.101 del 10 agosto 2018) che ha espressamente abrogato l'art. 29 del D.lgs 196/2003, è consigliabile **limitarsi alle sole nomine autorizzato del trattamento** seguendo le modalità predette in quanto par essere una figura non più prevista nel nostro ordinamento.
A prescindere dalle nomine formali, tuttavia, sarebbe opportuno organizzare per il personale **appositi corsi di formazione** con il fine di far comprendere i concetti del Regolamento e porre in essere condotte corrette e rispettose dei principi fondamentali dello stesso.
La formazione deve essere finalizzata ad illustrare i rischi generali e specifici connessi al trattamento dei dati personali, le misure organizzative, tecniche ed informatiche da adottare, nonché le responsabilità e le sanzioni, presentando un taglio sia interdisciplinare che pratico.
Per di più, una parte della dottrina considera la formazione del personale un **obbligo** a carico del titolare in base ad un'interpretazione letterale degli artt. 32. par. 4 e 39. par. 1 let b del regolamento e, pertanto, nel caso di mancata erogazione, potrebbe rientrare tra le casistiche sanzionatorie contemplate dall'art. 83 para. 4 che prevedono sanzioni amministrative fino a 10 milioni di euro o fino al 2% del fatturato.
Ciò posto, l' AZIENDA AGRICOLA MERRA PIERLUIGI è tenuta a pianificare un percorso di formazione per il proprio personale dipendente in base alle risorse disponibili. Difatti, è importante evidenziare che le nomine formali dei dipendenti sono prive di valore qualora il titolare, in fase ispettiva, non riesca a comprovare che a tutto il personale dipendente interessato al trattamento di dati siano state impartite le necessarie istruzioni e abbia avuto la necessaria formazione.

3. SOGGETTI TERZI E RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

Discorso differente riguarda i **soggetti esterni all'azienda** che svolgono servizi ed elaborano i dati per conto di quest'ultima. Difatti, in molti casi il titolare delega all'esterno lo svolgimento di alcune attività (outsourcing) o si avvale comunque di servizi che comportano, da parte del soggetto esterno, un trattamento di dati personali. Nel caso in esame si pensi ai tecnici che si occupano della manutenzione dei sistemi informatici, ai consulenti economico-aziendali, al consulente del lavoro che elabora le buste paga o alle aziende di trasporti.
Orbene, questa categoria di soggetti rientra, più opportunamente, nella definizione di responsabili (esterni) del trattamento ai sensi dell'art. 28 del GDPR e, pertanto, **sarà necessario documentare l'esistenza del rapporto tra titolare e responsabile con un apposito contratto o atto giuridico** che "*vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*" (Cfr art. 28 par.3 GDPR).

Il regolamento fissa dettagliatamente le caratteristiche dell'accordo stabilendo che lo stesso deve prevedere che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un obbligo legale di riservatezza;
c) adotti tutte le misure di sicurezza richieste ai sensi dell'art. 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) assista il titolare all'obbligo di dar seguito alle richieste per l'esercizio dei diritti;
f) cancelli o restituisca tutti i dati personali dopo che è terminata la prestazione:
g) consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto incaricato.

In pratica, con tale accordo il titolare delega al responsabile la concreta gestione del trattamento, affidandogli uno o più compiti specifici oppure una serie di compiti dettagliati in generale.

Il titolare del trattamento rimane garante della gestione effettuata dai responsabili del trattamento dovendo assicurare che le loro decisioni siano conformi alle leggi. Per questo motivo, il titolare in fase di scelta dei fornitori e dei consulenti è tenuto a valutare le garanzie offerte dagli stessi preoccupandosi di individuare responsabili del trattamento che offrano garanzie sufficienti ed adeguate nell'adozione di idonee misure tecniche e organizzative volte alla protezione dei dati personali.

A riguardo, la verifica delle credenziali può essere attuata anche attraverso l'esame dei codici di condotta o dei meccanismi di certificazione cui gli stessi aderiscono. (Cfr. par. 5).

Ciò nonostante, è opportuno considerare che nel caso in cui il responsabile del trattamento non adempie agli obblighi del Regolamento specificatamente diretti alla sua figura o agisce in modo difforme rispetto alle istruzioni del titolare, il responsabile risponde per i danni causati agli interessati (Cfr. art. 82 GDPR).

4. MISURE DI SICUREZZA

Qualsiasi operazione di trattamento di dati personali è legata indissolubilmente alla possibilità che si verifichino particolari situazioni dannose quali la distruzione, perdita, modifica non autorizzata, divulgazione non autorizzata e accesso non autorizzato ai dati personali causati sia da eventi accidentali sia da atti criminosi. Al fine di ridurre o possibilmente azzerare tali situazioni di rischio è opportuno predisporre ed attuare appropriate **misure di carattere tecnico** ed **organizzativo** all'interno della struttura aziendale**.**

In particolare, l'AZIENDA AGRICOLA MERRA PIERLUIGI tratta i dati personali **sia con strumenti/archivi cartacei sia con strumenti/archivi informatici** e, dunque, sono necessari differenti accorgimenti in base ai metodi utilizzati per la raccolta e la gestione del dato.

Preliminarmente, è essenziale mettere a punto una politica di controllo degli accessi ai documenti cartacei e informatici che vengono utilizzati per trattare i dati personali. **Il principio di base è limitare l'accesso solamente al personale specificatamente incaricato.** Tuttavia, anche i dipendenti incaricati devono essere istruiti in modo da accedere solamente ai dati necessari per svolgere il compito affidato evitando il contatto con altri dati non necessari, secondo il principio di minimizzazione illustrato all'art. 5, par. 1, let. C del Regolamento.

Per ciò che concerne la **documentazione cartacea** contenente dati personali è importante attuare una corretta politica di conservazione e utilizzo al fine di evitare la divulgazione o la dispersione dei dati.
A riguardo è importante osservare le seguenti precauzioni:

- I documenti cartacei contenenti dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali e, nell'ipotesi in cui questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- per tutto il periodo in cui i documenti contenenti dati personali sono al di fuori dei locali individuati per la loro conservazione, non devono mai essere lasciati incustoditi;
- i documenti contenenti dati personali trattati non devono essere esposti nelle postazioni durante l'orario di lavoro;
- al termine del loro utilizzo tutti i documenti contenenti dati personali devono essere riportati nei locali individuati per la loro conservazione;
- gli incaricati devono evitare che terzi possano accedere ai luoghi in cui sono custoditi i dati, quindi devono adottare misure idonee per evitare la visibilità dei dati a terzi;
- per ridurre il rischio di diffusione si deve limitare l'utilizzo di copie fotostatiche a quanto strettamente necessario.

Peraltro, maggiori cautele devono essere osservate nel trattamento dei **dati idonei a rilevare lo stato di salute** come i dati relativi ad infermità che determinano incapacità lavorativa temporanea (es. certificato medico per malattia o infortunio) che possono circolare anche con modalità cartacee ed essere custoditi nell'archivio generale.
Nello specifico, dette informazioni devono essere conservate separatamente da ogni altro dato personale dell'interessato in modo da non consentire una indistinta consultazione nel corso delle ordinarie attività amministrative. Sarebbe opportuno custodire i dati sanitari in apposite cartelle separate da quelle contenenti gli altri dati adottando, inoltre, i necessari accorgimenti al fine di impedire ogni accesso abusivo (es. buste sigillate, cassetti chiusi a chiave, cassaforte).
In riferimento agli accertamenti preventivi e periodici effettuati dal medico competente in materia di igiene e sicurezza dei luoghi di lavoro, ai sensi del D. Lgs. 626/1994 successivamente

riformato dal D.lgs 81/08, il solo medico è deputato a trattare i dati sanitari dei lavoratori procedendo alle dovute annotazioni nelle cartelle sanitarie e di rischio. Dette cartelle sono custodite presso l'azienda senza la facoltà del datore di lavoro di accedervi, difatti, il predetto non può conoscere le patologie ma solo la valutazione finale circa l'idoneità del dipendete allo svolgimento delle mansioni assegnate.

Importante, peraltro, risulta essere la sicurezza fisica dell'intera struttura aziendale e dell'archivio generale che se dotati di sistemi di protezione all'avanguardia sono il primo elemento di difesa da intrusioni indesiderate e da eventuali divulgazioni di dati personali.

In ultimo, particolare attenzione deve essere prestata nei casi in cui è necessario distruggere la documentazione contenente dati personali. Invero, per eliminare i rischi di diffusione di dati, è necessario utilizzare gli appositi **apparecchi "distruggi documenti**" idonei a frammentare i fogli in piccole unità in modo da renderli indecifrabili.

L' AZIENDA AGRICOLA MERRA PIERLUIGI è munita di tale strumentazione, ciò nonostante è opportuno verificare se vi è una prassi consolidata e rispettata da tutto il personale nell'utilizzare i distruggitori quando vi è necessità di eliminare la documentazione.

Invece, qualora sia necessario smaltire ingenti quantità di incartamenti è preferibile incaricare aziende specializzate nello smaltimento e distruzione dei documenti contenenti dati personali comuni e/o sensibili.

Per quanto concerne le misure di sicurezza degli **strumenti informatici** si rinvia alle considerazioni espresse nella sezione del presente documento denominata "VULNERABILITY ASSESSMENT".

5. CODICI DI CONDOTTA E MECCANISMI DI CERTIFICAZIONI

Il titolare del trattamento, ai sensi degli artt. 40 e 42 GDPR, per dimostrare e provare l'ottemperanza agli obblighi imposti dal Regolamento, può volontariamente aderire ai codici di condotta emanati dalle associazioni/organizzazioni rappresentanti le categorie a cui appartiene o a meccanismi di certificazione.

Tale adesione è fortemente consigliata in quanto, secondo una interpretazione dottrinale, è considerata una sorta di presunzione di "GDPR *compliance*" e ed è, peraltro, valutato positivamente in termini di *Impact Assessment*. Difatti, **sia i codici di condotta che i meccanismi di certificazione disciplinano il corretto e trasparente trattamento dei dati personali e consentono agli interessati di valutare il livello di protezione dei dati**.

L'aver aderito ad un codice di condotta o l'essersi certificato, però, **non libera totalmente il titolare né il responsabile del trattamento dalla responsabilità di conformità al Regolamento** e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti, compresi i poteri sanzionatori in casi di violazioni. Tuttavia, al momento di decidere se infliggere una sanzione amministrativa pecuniaria o fissare l'ammontare della stessa, le Autorità **terranno in conto anche dell'adesione ai codici di condotta** approvati ai sensi dell'articolo 40 o **ai meccanismi di certificazione** approvati ai sensi dell'articolo 42.

Ciò posto, in considerazione dei pochi mesi di attività del GDPR, ad oggi non esistono codici di condotta o meccanismi di certificazione approvati dall'Autorità Garante sulla base del Regolamento a cui l' AZIENDA AGRICOLA MERRA PIERLUIGI può aderire. **Sarà nostra cura informarvi tempestivamente non appena saranno disponibili codici di condotta o certificazioni, per l'ambito specifico di attività della vostra società.**

Peraltro, è importante segnalare che il decreto legislativo n. 101/2018 di adeguamento della normativa italiana al Gdpr ha specificato le tempistiche di convalida dei codici predetti che, comunque, non sembrano essere imminenti. Difatti, il decreto ha previsto che entro 6 mesi dalla data di entrata in vigore (19 settembre 2018), le imprese, le associazioni e gli altri organismi rappresentanti le categorie interessate devono sottoporre all'approvazione del Garante per la protezione dei dati personali i codici di condotta elaborati. Tale procedura, poi, deve concludersi entro 6 mesi successivi dalla sottoposizione del codice all'esame dell'Autorità Garante.

Come valida certificazione segnaliamo lo standard ISO/IEC 27001 che fornisce un framework comune, descrivendo i requisiti chiave per implementare un efficace sistema di gestione per la sicurezza delle informazioni, rappresentando un prezioso aiuto per garantire la conformità al GDPR.

Si tratta di una norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System) ed include aspetti relativi alla sicurezza logica, fisica e ed organizzativa. Difatti, la norma è stata creata al fine di garantire la sicurezza nella tecnologia dell'informazione e, di conseguenza, proteggere le informazioni sensibili in possesso dell'azienda da minacce di ogni tipo. Per tali ragioni, in attesa dell'approvazione di certificazioni specifiche in materia di protezione di dati personali, la conformazione alla ISO 27001 rappresenta un primo passo verso l'adozione di una corretta politica di protezione del dato personale e verso l'adesione a certificazioni approvate dall'Autorità Garante.

Si specifica, però, che l'eventuale conformità alla ISO 27001 non solleva l'organizzazione dal rispetto delle misure di sicurezza e dalla produzione della documentazione richiesta dalla legge sulla privacy.

9. REGISTRO DEI TRATTAMENTI

La tenuta del registro dei trattamenti, prevista dall'art. 30 del Regolamento, è una delle novità e, al contempo, uno degli adempimenti più importanti concernenti le attività di

trattamento dei dati personali. L'onere della tenuta è posto a carico del titolare e, se nominato, dal Responsabile (esterno) del trattamento che deve appuntare in un autonomo registro tutte le categorie di attività relative al trattamento svolto per conto del titolare (par. 2 art. 30 GDPR).

Il registro può essere redatto sia in formato cartaceo che in formato elettronico e dovrà contenere una serie di specifiche informazioni elencate nel par. 1 dell'art. 30:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali con l'indicazione delle eventuali garanzie adeguate prescritte;
- laddove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- laddove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

Tale registro, ai sensi del par. 4 dell'art. 30, dovrà essere messo a disposizione dell'Autorità Garante ogni qual volta lo richieda.
Inoltre, l'obbligo di redazione e adozione non è generale e, difatti, ai sensi del par. 5 art. 30, sono esentate le imprese o le organizzazioni con meno di 250 dipendenti, a meno che il trattamento effettuato:

- possa presentare un rischio per i diritti e le libertà degli interessati,
- non sia occasionale,
- o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 (cioè dati sensibili o giudiziari).

A riguardo, il Working Party Article 29 (il gruppo di lavoro comune europeo delle autorità nazionali di vigilanza e protezione dei dati), in una interpretazione dell'articolo in questione (documento interpretativo del 19 aprile 2018), ha precisato che è sufficiente una sola delle condizioni previste dall'articolo 30 per far scattare l'obbligo di tenuta del registro. Seguendo tali indicazioni, si noti che la maggior parte delle aziende tratta dati relativi alla salute dei dipendenti (ex dati sensibili) o anche un sito web con un *form* di contatti configura un trattamento di dati in maniera non occasionale.

In concreto, allora, la sola ipotesi in cui si possa ritenere escluso l'obbligo di cui si discute è quello di una piccola realtà aziendale o professionale o di un piccolo ente che effettui solamente un trattamento occasionale di dati comuni.

Tale orientamento, peraltro, è stato corroborato e precisato dall'Autorità Garante per la protezione dei dati personali attraverso la recente FAQ sul registro delle attività di trattamento (pubblicata in data 8 ottobre 2018) con la quale ha elencato, a titolo esemplificativo, una serie di piccole attività economiche e soggetti tenuti comunque a predisporre il registro dei trattamenti, tra cui si indicano:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.)
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- il condominio ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Dunque, sulla scorta delle indicazioni fornite dall'Autorità, pochissimi soggetti sarebbero esclusi dall'obbligo di redazione e tenuta del registro, difatti è raro imbattersi in attività economiche nella cui organizzazione aziendale non vi è presenza di alcun dipendente o non trattano dati compresi nelle categorie particolari di dati personali.

Tuttavia, l'Autorità precisa che "*le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento)*".
Alla luce di quanto suesposto, in considerazione del fatto che l'AZIENDA AGRICOLA MERRA PIERLUIGI si serve di personale dipendente di cui tratta anche dati inerenti la salute ed ha un costante flusso di dati provenienti da altri soggetti, è tenuto ad adottare il registro dei trattamenti seguendo le indicazioni sopra riportate.

Ciò nonostante, a prescindere dalla obbligatorietà o meno, in considerazione della tipologia di informazioni contenute, il registro risulta essere uno strumento fondamentale non soltanto per disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda, ma è anche funzionale alla corretta attuazione dei vari adempimenti prescritti dal Regolamento.

Difatti, in caso di ispezione da parte del Garante, la corretta tenuta del registro dimostrerà una profonda attenzione da parte dell'azienda alle tematiche di protezione dei dati personali e costituirà un buon biglietto da visita in tutte le tipologie di indagini o valutazioni dell'autorità.
Invero, la stessa Autorità, nella Guida all'applicazione del Regolamento pubblicata sul suo sito internet, considera il registro non un mero adempimento formale bensì un'attività che risulta essere parte integrante di un sistema di corretta gestione dei dati personali.
Quindi, si può sostenere che non vi sono vantaggi oggettivi dalla mancata tenuta del registro considerando, inoltre, che la compilazione risulta essere un impegno *una tantum* che non influisce sull'attività lavorativa.

7. DATA BREACH E VIOLAZIONE DEI DATI PERSONALI

Il data breach o "violazione dei dati personali" è definito dall'art. 4 n. 12 come <<la violazione di sicurezza che comporta 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>>.
A titolo esemplificativo, rientra nella definizione di data breach anche il semplice smarrimento di una cartellina o di una penna USB contenente dati personali oltre che un attacco ai sistemi informatici.
In questi casi sussistono obblighi specifici che presuppongono una previa e puntuale organizzazione da parte dell'azienda per il loro adempimento.
Difatti, ai sensi dell'art. 33 del Regolamento, l'azienda **dovrà notificare la violazione all'autorità di controllo competente (Garante della privacy) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza, ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati** (Cfr. considerando 85 del Regolamento). Se la notifica all'autorità di controllo viene effettuata dopo questo termine, la tardiva comunicazione deve essere corredata da un'ampia e convincente illustrazione dei motivi del ritardo.

L'obiettivo di tale comunicazione è chiaramente quello di consentire al Garante Privacy di attivarsi il prima possibile, valutare tempestivamente la gravità della situazione e stabilire le misure correttive da imporre al Titolare per ridurre al minimo i pericoli per la Privacy degli Interessati a cui si riferiscono i dati.

Ciò nonostante, è bene ricordare come la notifica all'autorità non sia obbligatoria, essendo subordinata ad una valutazione del rischio per gli interessati che spetta al titolare del trattamento. Se la violazione presenta rischi elevati per i diritti e le libertà delle persone fisiche coinvolte, si dovranno informare della violazione anche gli interessati con un'apposita **comunicazione**, sempre "senza ingiustificato ritardo"(art.34GDPR).

La notifica all'autorità di controllo, effettuata in modo chiaro e specifico, dovrà avere il contenuto previsto dall'art. 33 del Regolamento ossia:

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

In ogni caso, l' AZIENDA AGRICOLA MERRA PIERLUIGI, titolare del trattamento, dovrà opportunamente documentare le violazioni di dati personali subite tramite un apposito **registro delle violazioni**, anche se non comunicate alle autorità di controllo, nonché le conseguenze e i provvedimenti adottati. Il titolare dovrebbe anche documentare nel registro le ragioni delle decisioni assunte nei casi in cui non ha proceduto o ha ritardato la notifica e nel l'ipotesi in cui non ha comunicato la violazione agli interessati.

Tale documentazione dovrà essere fornita al Garante in caso di accertamenti.

Infine, si tenga presente che in caso di mancato rispetto delle procedure di notifica delle violazioni saranno applicate le sanzioni amministrative fino ad un massimo di 10 milioni di euro previste dall'art. 83 del Regolamento.

8. DATA PROTECTION OFFICER (DPO)

L'introduzione del **Responsabile per la protezione dei dati** *(data protection officer o DPO)* è una delle principali e più significative innovazioni del Regolamento. Si **tratta di una figura altamente specializzata con conoscenze approfondite della normativa e delle prassi in materia di protezione dati, nonché delle procedure amministrative che caratterizzano lo specifico settore di riferimento.** Il DPO, sostanzialmente, svolge un duplice compito: da un lato informa e fornisce consulenza al titolare ed al responsabile del trattamento in merito agli obblighi in materia di *data protection*; dall'altro funge da raccordo tra il titolare o il responsabile del trattamento e l'autorità Garante.

Nello specifico deve:

- informare e fornire consulenza al titolare e al responsabile del trattamento nonché ai dipendenti del sorvegliare l'osservanza del regolamento, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati;
- obblighi derivanti dal regolamento;

- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;
- fornire pareri e sorvegliare alla redazione della Data protection impact assessment (c.d. Dpia);
- fungere da punto di contatto e collaborare con l'Autorità Garante per la protezione dei dati personali;
- controllare che le violazioni dei dati personali siano documentate, notificate e comunicate

Sono obbligati alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett.a), b) e c), del Regolamento ossia ogniqualvolta:

a) *il trattamento è effettuato da autorità pubblica o organismo pubblico, ad eccezione delle autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;*
b) *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;*
c) *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 dati relativi a condanne penali e a reati di cui all'art.10.*

Il Garante, nella FAQ del 26/03/2018 per il settore privato, fornisce utili precisazioni individuando dei casi pratici in cui la nomina del DPO deve considerarsi doverosa e circostanze in cui la nomina non è necessaria. Tra i soggetti non obbligati alla nomina del DPO, l'Autorità individua "le piccole e medie imprese con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti".

L' AZIENDA AGRICOLA MERRA PIERLUIGI effettua attività di trattamento dati personali quasi esclusivamente nei confronti dei dipendenti e dei fornitori poiché la clientela è caratterizzata, in prevalenza, da società di capitali che, come esplicitato in premessa, non rientrano nel novero dei soggetti tutelati dalla disciplina del Regolamento europeo n. 679/2016.

Pertanto, l'azienda in esame non è assoggettata all'obbligo di nomina del DPO, tuttavia in considerazione della struttura organizzativa e del costante flusso di dati presente all'interno dell'azienda si consiglia la designazione.

Difatti, tale nomina, anche se non obbligatoria, inserendosi nella logica di responsabilizzazione (accountability) del titolare del trattamento, dimostrerebbe all'Autorità di controllo, in caso di ispezioni, la piena conformità dell'organizzazione aziendale alle regole ed ai principi del Regolamento.

Il DPO potrà essere scelto tra un soggetto interno o esterno e autonomo all'azienda, ingaggiato con un apposito contratto di servizio. Importante, in tal senso, **è scegliere un profilo con un grado di professionalità adeguato alla complessità del compito da svolgere e alle responsabilità da sostenere e che non sia in conflitto d'interesse con**

Quest'ultimo, difatti, è chiamato a svolgere in autonomia valutazioni molto importanti (*risk-based*) sui rischi del trattamento di dati che l'azienda intende effettuare e, conseguentemente, sulle scelte operative ed organizzative che ne discendono.
Infine, si tenga presente che il nominativo del DPO incaricato dovrà essere comunicato all'Autorità Garante attraverso una procedura online presente sul sito www.garanteprivacy.it. Tale procedura è l'unica utilizzabile per l'invio dei dati di contatto del Responsabile della protezione dei dati e non saranno prese in considerazione le comunicazioni effettuate attraverso diversi canali di contatto con il Garante (es. e-mail, posta, ecc.).

9. DIRITTI DELL'INTERESSATO

Il regolamento attribuisce specifici diritti all'interessato il quale può rivolgersi direttamente al titolare del trattamento per l'esercizio. A riguardo, è importante sottolineare che l'interessato può esercitare tali diritti in qualsiasi momento e quindi anche in un momento successivo a quello in cui si è prestato il consenso.
I diritti esercitabili dall'interessato sono disciplinati dagli artt. 15- 21 del Regolamento e sono i seguenti:

- Diritto di opposizione al trattamento
- Diritto di cancellazione (diritto all'oblio) dei dati in possesso del titolare;
- Ottenere l'aggiornamento o la rettifica dei dati conferiti;
- ottenere in forma intellegibile i dati in possesso del titolare (diritto di accesso);
- diritto di limitazione del trattamento;
- diritto alla portabilità;

Per garantire l'esercizio dei suesposti diritti, è opportuno che l'azienda adotti tutte le misure tecniche e organizzative necessarie per favorire l'esercizio degli stessi e il riscontro alle richieste presentate dagli interessati che dovranno essere presentate in forma scritta (anche elettronica). A titolo esemplificativo, l'AZIENDA AGRICOLA MERRA PIERLUIGI potrebbe predisporre un'apposita casella e-mail per ricevere tali richieste e per provvedere al riscontro.

Una volta che l'interessato richiede l'esercizio dei diritti, l'azienda deve rispondere alle richieste "senza ingiustificato ritardo "o comunque entro 1 mese dalla richiesta, estendibili fino a 3 mesi solo nei casi di particolare complessità. Il titolare deve fornire sempre riscontro all'interessato entro il termine precedentemente indicato, anche in caso di diniego, però in questo caso motivando la decisione di non accogliere la richiesta.
Infine, è importante sottolineare come l'esercizio di tali diritti è, in linea di principio, gratuito per l'interessato tranne nei casi in cui le richieste siano manifestamente infondate o eccessive ovvero sono richieste più copie dei dati personali.