MANUALE SULLA GESTIONE E TRATTAMENTO DEI DATI

AI SENSI DEL REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 27 APRILE 2016 E DELLE RELATIVE DISPOSIZIONI DI ADEGUAMENTO DISCIPLINATE DAL D.LGS DEL 10 AGOSTO 2018, N. 101

Azienda	Società Agricola Semplice Belmonte di Mazzilli Rosa Anna
Sede Legale	Via Pitagora, 30 - 70033 Corato (BA)
Sede Operativa	S.P. 231 SC Parco del Fornello - 70037 Ruvo di puglia (BA)

Rev.	Motivazione	Data	Emissione a cura di	Revisione e controllo a cura del Responsabile del Trattamento
00	Emissione ed aggiornamento al GDPR	10/08/2020	Società Agricola Semplice Belmonte di Mazzilli Rosa Anna	Sig.ra Mazzilli Rosa Anna
01				
02				
03				
04				
05				

Indice

PARTE 1 – INDICAZIONI GENERALI

1. PREMESSA – Introduzione al GDPR ... 3
2. DEFINIZIONI ... 4
3. TRATTAMENTO DEI DATI ... 7
4. LICEITÀ DEL TRATTAMENTO (ART.6) ... 10
5. CONDIZIONI PER IL CONSENSO (ART.7) ... 12
6. DIRITTI DEGLI INTERESSATI ... 12
6.1 Diritto di accesso (ART. 15) ... 13
6.2 Diritto di rettifica (ART. 16) ... 13
6.3 Diritto di cancellazione (diritto all'oblio) (ART. 17) ... 13
6.4 Diritto di limitazione del trattamento (ART. 18) ... 13
6.5 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (ART.19) ... 14
6.6 Diritto alla portabilità dei dati (ART. 20) ... 14
6.7 Diritto di opposizione (ART. 21) ... 14
7. Approccio basato sul rischio e misure di accountability di titolari e responsabili ... 16
7.1 Registro dei trattamenti (ART. 30) ... 17
7.2 DPIA – DATA PROTECTION IMPACT ASSESSMENT ... 18
7.3 Notifica di violazione dei dati ... 23
7.4 Criteri e modalità per il ripristino della disponibilità dei dati ... 24
7.5 Altre misure di sicurezza ... 25
7.6 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari ... 25
7.7 Trattamenti senza l´ausilio di strumenti elettronici ... 26
8. DATA BREACH ... 27
9. TITOLARE, RESPONSABILE, INCARICATO AL TRATTAMENTO ... 28
9.1 Il titolare del trattamento – Le responsabilità (ART. 24) ... 28
9.2 CONTITOLARITA' DEL TRATTAMENTO ... 28
9.3 Il responsabile del trattamento dati (ART. 28) ... 29
9.4 Designazione del responsabile della protezione dei dati (ART. 37) ... 30
10. INFORMATIVA ... 32
10.1 Contenuti dell'informativa ... 32

10.2 Tempi dell'informativa 32
10.3 Modalità dell'informativa 32
11. TRASFERIMENTI DI DATI VERSO PAESI TERZI E ORGANISMI INTERNAZIONALI 36
12. REGOLE FONDAMENTALI PER LA CONFORMITÀ DI UN SITO WEB 37
12.1 GDPR e Sito Web: diritto alla cancellazione dei dati personali 37
12.2 GDPR e Sito Web: registrazione dei Log 37
12.3 GDPR e Sito Web: I diritti dell'interessato 38
12.4 GDPR e Sito Web: il diritto di essere informato 38
12.5 GDPR e Sito Web: la newsletter 38
12.6 GDPR e Sito Web: la gestione dei dati personali 39
13. SANZIONI 39

PARTE 2 – SEZIONE OPERATIVA

1 PRESENTAZIONE AZIENDA 40
2 ANALISI DEL CICLO PRODUTTIVO E DEI PROCESSI 41
3 TIPOLOGIA E TRATTAMENTO DATI 47
4 GUIDA ALL'UTILIZZO DEL MANUALE DELLA PRIVACY 77

PARTE 1 – Indicazioni generali

1. PREMESSA– Introduzione al GDPR

La struttura del presente documento viene redatta per descrivere le modalità di adozione delle misure di sicurezza ai sensi del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 nonché ai sensi delle relative disposizioni di adeguamento disciplinate dal D.Lgs del 10 agosto 2018, n. 101.

La redazione del presente documento è stata incentrata sulla possibilità di rendere uno strumento efficace ed operativo, pertanto in prima analisi viene fornita una panoramica relativa ai riferimenti normativi ed adempimenti, successivamente il manuale definisce le prassi pratiche tali da diventare un essenziale metodo operativo.

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'art. 8, paragrafo 1, della Carta dei Diritti Fondamentali dell'Unione Europea e l'art. 16, paragrafo 1, del Trattato sul Funzionamento dell'Unione Europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il Regolamento Europeo n. 2016/679 è inteso a 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.

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 in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

Il presente manuale ha l'obiettivo di attestare la conformità delle misure organizzative e di sicurezza in conformità di quanto definito dalla legge.

2. DEFINIZIONI

Ai fini del Regolamento (UE) 2016/679 s'intende per:

1) **«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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) **«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;
3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) **«profilazione»:** qualsiasi forma di trattamento automatizzato di dati personali consistente nel l'utilizzo di tali dati personali per valutare determinati aspetti personali relativi auna persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5) **«pseudonimizzazione»:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6) «**archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7) **«titolare del trattamento»**: 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 di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8) **«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;
9) **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da

parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) **«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 al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11) **«consenso dell'interessato»:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
12) **«violazione dei dati personali»**: 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;
13) **«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;
14) **«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;
15) **«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;
16) **«stabilimento principale»**:
    1) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
    2) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente Regolamento;
17) **«rappresentante»**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'arti. 27 del Regolamento (UE) 2016/679, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente Regolamento;

18) **«impresa»**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
19) **«gruppo imprenditoriale»**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
20) **«norme vincolanti d'impresa»**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
21) **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51;
22) **«autorità di controllo interessata»**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    1) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
    2) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
    3) un reclamo è stato proposto a tale autorità di controllo;
23) **«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;
    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 incide in modo sostanziale su interessati in più di uno Stato membro;
24) **«obiezione pertinente e motivata»**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente Regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
25) **«servizio della società dell'informazione»**: il servizio definito all'articolo 1, paragrafo1, lettera b), della Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
26) **«organizzazione internazionale»**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3. TRATTAMENTO DEI DATI

Il trattamento dei dati viene effettuato con l'adozione di misure idonee a garantirne la sicurezza e la riservatezza, sia mediante strumenti elettronici, sia con modalità cartacea.

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all' art. 5 del Regolamento (UE) 2016/679, che qui si riportano:

1) liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
2) limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
3) minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
4) esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
5) limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
6) integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Secondo l'art.5, paragrafo 2 il titolare del trattamento deve rispettare tutti questi principi ed essere "in grado di comprovarlo". Il titolare deve 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 (Principio di Responsabilizzazione).

Il Regolamento pone l'accento sulla "responsabilizzazione" di titolari e responsabili, ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (artt. 23-25, in particolare, e l'intero Capo IV del Regolamento).

Dunque, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Quando il trattamento si fonda sul consenso dell'interessato, il titolare deve sempre essere in grado di dimostrare (art. 7.1) che l'interessato ha prestato il proprio consenso, che è valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali;
- è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre revocabile.

Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno della modulistica.

Non è ammesso il consenso tacito o presunto (per esempio, presentando caselle già spuntate su un modulo).

Quando il trattamento riguarda le "categorie particolari di dati personali" (art. 9) il consenso deve essere "esplicito"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art.22).

Il consenso non deve essere necessariamente documentato per iscritto, né è richiesta la forma scritta, anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere esplicito (per le categorie particolari di dati di cui all'art.9).

L'informativa deve essere di forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee. Deve essere data, in linea di principio, per iscritto e preferibilmente in formato elettronico, anche se sono ammessi altri mezzi, quindi può essere fornita anche oralmente.

Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione dei dati. Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo in combinazione con l'informativa estesa; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

L'interessato ha le seguenti facoltà:

1) chiedere se esistono dati che lo riguardano e come vengono utilizzati (diritto di accesso);
2) se necessario, richiedere l'aggiornamento, la rettifica o l'integrazione dei suoi dati;
3) chiedere di provvedere alla cancellazione dei dati personali ("diritto all'oblio");
4) chiedere di limitare o bloccare i dati trattati in eventuale violazione di legge;
5) ove tecnicamente possibile, chiedere di ottenere copia dei suoi dati in un formato interoperabile facilmente trasferibile ad altro operatore;
6) fare opposizione, per motivi legittimi, all'utilizzo dei suoi dati;
7) revocare il consenso prestato in ogni momento;
8) chiedere informazione circa l'esistenza di un processo decisionale basato unicamente su di un trattamento automatizzato.

Le modalità per limitare il trattamento dei dati personali possono consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali deve essere in linea di massima assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati.

Per rafforzare ulteriormente il controllo sui propri dati è opportuno che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere, in un formato strutturato e leggibile da dispositivo automatico e interoperabile, i dati personali che lo riguardano, forniti a un titolare del trattamento, e di trasmetterli a un altro titolare del trattamento.

È opportuno, da parte dei titolari del trattamento, sviluppare formati interoperabili che consentano la portabilità dei dati. Tale diritto deve essere applicato qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto.

Il diritto alla portabilità del dato non deve applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non deve pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non deve pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente Regolamento. Inoltre tale diritto non deve pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le relative limitazioni di cui al presente Regolamento e non deve segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto. Ove tecnicamente fattibile, l'interessato deve avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento ad un altro.

4. LICEITÀ DEL TRATTAMENTO (ART.6)

1. Ai sensi dell'art.6 del Regolamento (UE) 2016/679 il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
   a) l'interessato ha espresso il consenso al trattamento dei dati personali per una o più specifiche finalità;
   b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   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 degli 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 interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento.

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:
   a) dal diritto dell'Unione, oppure;
   b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui:

   a) le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento;
   b) le tipologie di dati oggetto del trattamento;
   c) gli interessati;

d) i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati.

Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri, che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'art. 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:
   - di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
   - del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
   - della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'art. 10, delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
   - dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

5. CONDIZIONI PER IL CONSENSO (ART.7)

Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato abbia prestato il proprio consenso al trattamento dei dati personali.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di tale consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento stesso. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

6. DIRITTI DEGLI INTERESSATI

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del Regolamento (UE) 2016/679.

Il termine previsto per la risposta all'interessato è di 1 mese, per tutti i diritti (compreso il diritto di accesso), estendibile fino a 3 mesi in casi di particolare complessità; il titolare del trattamento dei dati deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere, ma soltanto se si tratta di richieste infondate o eccessive (anche ripetitive) (art.12, paragrafo 5), ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti.

Il riscontro all'interessato di regola deve avvenire in forma scritta, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, o in forma orale solo se richiesto dall'interessato stesso (art. 12, paragrafo 1; art. 15, paragrafo 3).

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (art. 15-22), il responsabile del trattamento dei dati è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)).

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Il titolare ha il diritto di chiedere informazioni necessarie ad identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.

Sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali.

6.1 Diritto di accesso (ART. 15)

Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento. Fra le informazioni che il titolare del trattamento deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

6.2 Diritto di rettifica (ART. 16)

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

6.3 Diritto di cancellazione (diritto all'oblio) (ART. 17)

Il diritto all'oblio si configura come un diritto alla cancellazione dei dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione". Inoltre è opportuno precisare come all'interessato è riconosciuto il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.

6.4 Diritto di limitazione del trattamento (ART. 18)

Diritto esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche nel caso in cui l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare del trattamento dei dati) o si oppone al loro trattamento ai sensi dell'art. 21 del Regolamento (UE) 2016/679 (in attesa della valutazione da parte del titolare). Esclusa la

conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante). Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che il titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

6.5 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (ART.19)

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'art. 6, dell'art.17, paragrafo 1, e dell'art.18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

6.6 Diritto alla portabilità dei dati (ART. 20)

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori. Non si applica ai trattamenti non automatizzati (non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono soggetti alla portabilità solo i dati trattati con il consenso o sulla base di un contratto stipulato con l'interessato (non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare del trattamento dei dati.

Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

6.7 Diritto di opposizione (ART. 21)

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'art. 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'art. 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

7. Approccio basato sul rischio e misure di accountability di titolari e responsabili

Il Regolamento (UE) 2016/679 pone grande attenzione sul concetto della "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili del trattamento dei dati – ossia, sull'adozione di comportamenti proattivi e sul dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "***data protection by default and by design***" ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" e tutelare i diritti degli interessati – considerando il contesto complessivo ove il trattamento si colloca, i rischi per i diritti e le libertà degli interessati.

Fondamentali fra le molteplici attività sono quelle connesse al rischio inerente il trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione considerando i rischi noti o evidenziabili e le misure tecniche e organizzative (anche di sicurezza). All'esito di questa valutazione il titolare potrà decidere in autonomia se iniziare il trattamento ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale. L'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, l'intervento delle Autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare. Peraltro, alle autorità di controllo, e in particolare al "Comitato Europeo della Protezione dei Dati" spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e documenti di indirizzo su queste e altre tematiche connesse, anche per garantire adattamenti necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

7.1 Registro dei trattamenti (ART. 30)

I dati personali, acquisiti tramite la procedura di notificazione telematica, sono trattati con modalità prevalentemente informatiche e telematiche ed inseriti in un registro elettronico dei trattamenti tenuto dal Garante, consultabile da chiunque anche per via telematica, oppure presso l'Autorità o soggetti pubblici convenzionati.

Le notizie accessibili tramite la consultazione del registro possono essere trattate, anche dai terzi che vi accedono, solo per finalità di applicazione della disciplina in materia di trattamento dei dati personali. In particolare, l'Autorità le utilizza per verifiche e controlli ed altre attività necessarie per svolgere i propri compiti istituzionali.

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti - ma solo se non effettuano trattamenti a rischio (art. 30, paragrafo 5 del Regolamento (UE) 2016/679) - devono mantenere un registro delle operazioni di trattamento.

Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. I contenuti del registro sono definiti nell'art. 30, tuttavia niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

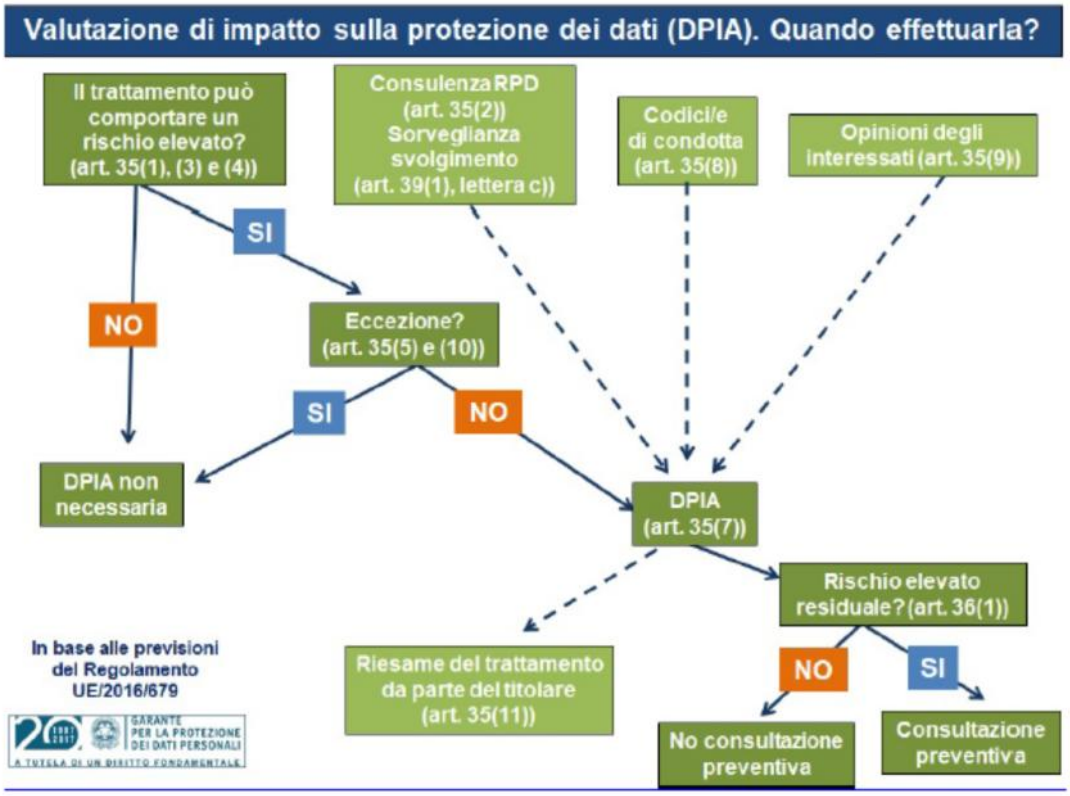
Il rischio non si riferisce al titolare ma al soggetto interessato e deve riguardare la sicurezza e gli aspetti complessivi del trattamento.

7.2 DPIA – DATA PROTECTION IMPACT ASSESSMENT

Procedura prevista dall'art. 35 del Regolamento (UE) 2016/679, la Data Protection Impact Assessment (D.P.I.A.) mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità ovvero i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Uno strumento importante in termini di responsabilizzazione (accountability) poiché aiuta il titolare del trattamento non solo a rispettare le prescrizioni del Regolamento in questione, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tale prescrizioni. Dunque tale procedura permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati. La DPIA deve essere condotta prima di procedere al trattamento, ma è previsto un riesame continuo ripetendo la valutazione ad intervalli regolari. La responsabilità del DPIA spetta al titolare del trattamento, anche se è possibile delegare tale mansione ad un soggetto, interno o esterno all'organizzazione. In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche questo strumento di responsabilizzazione risulta essere obbligatorio. Diversamente non risulta essere necessaria per i trattamenti:

1) quando non è probabile che il trattamento comporti "un alto rischio ai diritti e alle libertà delle persone fisiche";
2) quando la natura, l'ambito, il contesto e gli scopi del trattamento sono molto simili ai trattamenti per i quali è stata effettuata la DPIA. In tali casi, possono essere utilizzati i risultati delle DPIA per trattamenti simili;
3) quando le operazioni di trattamento sono state controllate da un'autorità di vigilanza prima del maggio 2018 in condizioni specifiche che non sono cambiate;
4) se un'operazione di trattamento ha una base giuridica nella legislazione dell'UE o dello Stato membro in cui la legge disciplina l'operazione di trattamento specifica e se una DPIA è già stata effettuata, salvo che uno Stato membro ritenga necessario effettuare una valutazione di impatto prima delle attività di trattamento;
5) se il trattamento è incluso nell'elenco facoltativo (stabilito dall'autorità di vigilanza) delle operazioni di trattamento per le quali non è richiesta la DPIA.

La valutazione di impatto sulla protezione dei dati (DPIA) risulta necessaria o meno seguendo il seguente flow-chart proposto dal "Garante della Protezione dei dati personali".

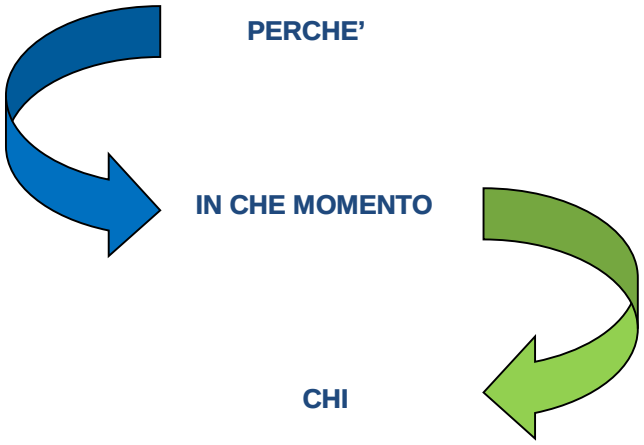


Quando e come applicare la DPIA, quali sono i soggetti interessati? Si propone pertanto la seguente rappresentazione grafica volta a chiarirne gli aspetti essenziali ed operativi.

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGDP)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.



PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT**.

La DPIA risulta pertanto obbligatoria o facoltativa? La schematizzazione che segue ne chiarisce gli aspetti di necessità ed obbligatorietà in relazione a quanto disposto dai riferimenti normativi vigenti.

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

L'applicazione del DPIA trova pertanto operatività all'interno della sezione dedicata e costituente l'elaborato tecnico del Registro dei Trattamenti. In apposito modulo dedicato si procede alla valutazione dei seguenti campi ed argomenti:

1) **Processo**: tipologia di processo oggetto di analisi;
2) **Descrizione sintetica dei processi e modalità di gestione**: descrizione delle modalità di gestione del processo di acquisizione, le stesse vengono definite prima dell'acquisizione di un dato;
3) **Valutazione richiesta e fase della valutazione**: si procede con la valutazione della necessità di avviare la DPIA e con conseguente stato della valutazione;
4) **Misure di prevenzione e protezione adottate**: procedure atte a prevenire il rischio ed al contempo contenerne gli effetti (magnitudo ovvero "impatto");
5) **Soggetto incaricato**: identificazione del soggetto interno e/o esterno incaricato, previa indicazione del Titolare del trattamento;
6) **Indicazione della Valutazione (DPIA)**: esiti dell'analisi effettuata;
7) **Riesame periodico**: identificazione della periodicità con la quale attuare l'analisi.

7.3 Notifica di violazione dei dati

Ai sensi dell'art. 33 (Notifica di una violazione dei dati personali all'Autorità di controllo) e dell'art. 34 (Comunicazione di una violazione dei dati personali all'interessato) il Regolamento (UE) 2016/679 disciplina i casi in cui il trattamento dei dati è soggetto a violazioni.

Tutti i titolari sono tenuti a notificare al Garante le violazioni di dati personali di cui vengano a conoscenza, entro **72 ore** e comunque "***senza ingiustificato ritardo***", se ritengono che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo" (art. 34, paragrafo 1); fanno eccezione le circostanze indicate dall'art. 34, paragrafo 3.

Tutti i titolari di trattamento devono in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (art.33, paragrafo 5). È bene, dunque, adottare le misure necessarie a documentare eventuali violazioni, anche perché i titolari sono tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

7.4 Criteri e modalità per il ripristino della disponibilità dei dati

In materia di protezione dei dati personali si delineano diverse misure minime di sicurezza:

Sistema di autenticazione informatica

1) Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di **credenziali di autenticazione** che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti;
2) Le credenziali di autenticazione consistono in un codice per l´identificazione dell´incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell´incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell´incaricato, eventualmente associata a un codice identificativo o a una parola chiave;
3) Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l´autenticazione;
4) Attraverso le istruzioni impartite agli incaricati è prevista l'adozione di cautele necessarie per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell´incaricato;
5) **La parola chiave**, quando è prevista dal sistema di autenticazione, è composta da almeno **otto caratteri** oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all´incaricato ed è modificata da quest´ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi;
6) Il codice per l´identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi;
7) Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
8) Le credenziali sono disattivate anche in caso di perdita della qualità che consente all´incaricato l´accesso ai dati personali;
9) Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
10) Quando l´accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della credenziale per l´autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell´incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l´incaricato dell´intervento effettuato;

11) Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione;
12) Sistema di autorizzazione: quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione;
13) I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all´inizio del trattamento, in modo da limitare l´accesso ai soli dati necessari per effettuare le operazioni di trattamento;
14) Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

7.5 Altre misure di sicurezza

1) Nell´ambito dell´aggiornamento periodico, con cadenza almeno annuale dell´individuazione dell´ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;
2) I dati personali sono protetti contro il rischio di intrusione e dell´azione di programmi di cui all´art. 615-quinquies del Codice Penale, mediante l´attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
3) Gli aggiornamenti periodici dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l´aggiornamento è almeno semestrale;
4) Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

7.6 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

1) I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all´art. 615-ter del Codice Penale, mediante l´utilizzo di idonei strumenti elettronici;
2) Sono impartite istruzioni organizzative e tecniche per la custodia e l´uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti;
3) I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili;

4) Sono adottate idonee misure per garantire il ripristino dell´accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;
5) Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati (con le modalità di cui all´ ex. art. 22, comma 6, del D.Lgs 196/2003), anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all´identità genetica sono trattati esclusivamente all´interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all´esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato;
6) Le misure di garanzia che riguardano i dati genetici e il trattamento dei dati relativi alla salute per finalità di prevenzione, diagnosi e cura sono adottate sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanità. Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'art. 9, paragrafo 4, del Regolamento (UE) 2016/679, o altre cautele specifiche. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

7.7 Trattamenti senza l´ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare del trattamento, del responsabile del trattamento, ove designato, e dell´incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

1) Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l´intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell´ambito dell´aggiornamento periodico con cadenza almeno annuale dell´individuazione dell´ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;
2) Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
3) L´accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l´orario di chiusura, sono identificate e registrate. Quando gli archivi non sono

dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

8. DATA BREACH

Il Regolamento (UE) 2016/679 introduce un nuovo obbligo consistente nella notifica, all'Autorità di controllo, di casi di violazione dei dati personali che presentano un rischio per i diritti e le libertà degli interessati.

Per violazione di dati personali si intende la distruzione, perdita, modifica, divulgazione non autorizzata l'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (art. 33 comma 2 del Regolamento).

La notifica non deve essere fatta qualora il titolare del trattamento ritenga sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica deve essere effettuata entro 72 ore dal momento in cui il titolare del trattamento è venuto a conoscenza della violazione. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

9. TITOLARE, RESPONSABILE, INCARICATO AL TRATTAMENTO

9.1 Il titolare del trattamento – Le responsabilità (ART. 24)

Il Regolamento (UE) 2016/679 disciplina la figura del titolare del trattamento dei dati, definita 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 di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

L'art. 24 definisce, a tal proposito, le responsabilità in considerazione della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento: il titolare del trattamento, dunque, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in modo conforme. Dette misure sono riesaminate e aggiornate qualora necessario.

Il Regolamento:

1) disciplina la contitolarità del trattamento (art. 26) e impone ai titolari del trattamento di definire specificamente, mediante un atto giuridicamente valido, il rispettivo ambito di responsabilità e i compiti con particolare riguardo all´esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente ad uno qualsiasi dei titolari operanti congiuntamente;
2) definisce in modo dettagliato le caratteristiche dell´atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto o di un atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile al trattamento al titolare che stipuli la materia disciplinata, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare (art. 28, paragrafo 3);
3) consente la nomina di sub-responsabili del trattamento da parte di un responsabile (art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest´ultimo risponde dinanzi al titolare dell´inadempimento dell´eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l´evento dannoso "non gli è in alcun modo imputabile" (art. 82, paragrafo 1 e paragrafo 3).

9.2 CONTITOLARITA' DEL TRATTAMENTO

Ai sensi dell'art. 26 del Regolamento (UE) 2016/679 due o più titolari del trattamento dei dati possono determinare congiuntamente le finalità ed i mezzi di trattamento, divenendo dunque "contitolari del trattamento". Questo caso viene regolamentato mediante un accordo interno dove i contitolari rendono espliciti le rispettive responsabilità in merito all'osservanza degli obblighi, con particolare attenzione all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

L'accordo, messo a disposizione dell'interessato, deve riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. L'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento. Tale accordo può risultare utile per alcuni tipi di gruppi societari dove ci sono risorse condivise per ottimizzare i costi.

9.3 Il responsabile del trattamento dati (ART. 28)

Il responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, comma 8 del Regolamento (UE) 2016/679 - definizioni).

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre ad un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, 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.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

1) tratti i dati personali solo su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
2) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
3) adotti tutte le misure richieste ai sensi dell'art. 32 (Sicurezza del trattamento);
4) rispetti le condizioni per ricorrere a un altro responsabile del trattamento;

5) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
6) assista il titolare del trattamento nel garantire il rispetto degli obblighi, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
7) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
8) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi definiti, contribuendo alle attività di revisione (comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato). Il responsabile del trattamento è tenuto ad informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando un responsabile del trattamento ricorre a un altro responsabile per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, sul responsabile del trattamento (nominato successivamente) sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora il responsabile del trattamento nominato successivamente ometta l'adempimento ai propri obblighi, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

9.4 Designazione del responsabile della protezione dei dati (ART. 37)

1) Il titolare del trattamento ed il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
   a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le 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;
   oppure
   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 (art. 9 del Regolamento (UE) 2016/679 - Trattamento di categorie particolari di dati personali) o di dati relativi a condanne penali e

a reati (art. 10 del Regolamento (UE) 2016/679 - Trattamento dei dati personali relativi a condanne penali e reati).

2) Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che uno di essi sia facilmente raggiungibile da ciascuno stabilimento.
3) Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, considerando la loro struttura organizzativa e dimensione.
4) Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa, delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di (art. 39 del Regolamento (UE) 2016/679 - Compiti del responsabile della protezione dei dati).
5) Il responsabile della protezione dei dati 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.
6) Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

10. INFORMATIVA

10.1 Contenuti dell'informativa

Ai sensi degli artt. 13, paragrafo 1, e 14, paragrafo 1, del Regolamento(UE) 2016/679 il titolare del trattamento deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.

Il Regolamento (UE) 2016/679 prevede inoltre ulteriori informazioni in quanto "**necessarie per garantire un trattamento corretto e trasparente**": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'Autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'Informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Tra i contenuti dell'Informativa non bisogna sottovalutare l'acquisizione di informazioni mediante altre fonti. Ad esempio è possibile l'utilizzo di fonti pubbliche di dati per supportare le funzionalità di eventuali siti web (tra cui le verifiche di autenticazione e antifrode) e/o per monitorare l'esattezza dei dati in possesso.

10.2 Tempi dell'informativa

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del Regolamento (UE) 2016/679), l'Informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).

10.3 Modalità dell'informativa

Il Regolamento (UE) 2016/679 specifica come l'Informativa deve avere una forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; per cui occorre utilizzare un linguaggio chiaro e semplice, e per i minori è opportuno prevedere informative idonee.

L'Informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: anche se sono ammessi "altri mezzi"; quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche delineate). È ammesso l'utilizzo di icone per presentare i contenuti

dell'informativa stessa in forma sintetica (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'UE e saranno definite prossimamente dalla Commissione Europea.

Ai sensi dell'art. 13 del Regolamento (UE) 2016/679 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato: della protezione dei dati, ove applicabile;

a) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
b) qualora il trattamento si basi sull'art. 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
c) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.

1) In riferimento al punto 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni che risultano essere necessarie per garantire un trattamento corretto e trasparente:
   a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per definirlo;
   b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   c) qualora il trattamento sia basato sull'art. 6, paragrafo 1, lettera a), oppure sull'art. 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   d) il diritto di proporre reclamo a un'Autorità di controllo;
   e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
   f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2) Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale trattamento ulteriore fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
3) I punti 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Ai sensi dell'art. 14 del Regolamento (UE) 2016/679 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato:

1) Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce a quest' ultimo le seguenti informazioni:
   a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso di trasferimenti dei dati, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2) Oltre alle informazioni di cui al punto 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
   a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   b) qualora il trattamento si basi sull'art. 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
   c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   d) qualora il trattamento sia basato sull'art. 6, paragrafo 1, lettera a), oppure sull'art. 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
   e) il diritto di proporre reclamo a un'Autorità di controllo;
   f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
   g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3) Il titolare del trattamento fornisce le informazioni fino ad ora citati:
   a) entro un termine ragionevole dall'ottenimento dei dati personali, oppure entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
   b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al momento della prima comunicazione all'interessato; oppure
   c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

4) Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al punto 2.

5) I punti da 1 a 4 non si applicano se e nella misura in cui:
   a) l'interessato dispone già delle informazioni;
   b) comunicare tali informazioni risulta impossibile o comporterebbe uno sforzo sproporzionato;
   c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro a cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
   d) qualora i dati personali debbano rimanere riservati nel rispetto del segreto professionale, disciplinato dal diritto dell'Unione o degli Stati membri, compreso l'obbligo di segretezza previsto per legge.

11. TRASFERIMENTI DI DATI VERSO PAESI TERZI E ORGANISMI INTERNAZIONALI

Il Regolamento (UE) 2016/679 consente di ricorrere anche a codici di condotta ovvero a schemi di certificazione per dimostrare le "**garanzie adeguate**" (art. 46). Ciò significa che i titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. Tuttavia, secondo gli artt. 40, paragrafo 3 e 42, paragrafo 2), tali titolari dovranno assumere, inoltre, un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento che sia giuridicamente vincolante e azionabile dagli interessati.

Sono vietati i trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (art. 48). É possibile far riferimento, tuttavia, ad altri presupposti e in particolare a deroghe previste per situazioni specifiche citate nell'art. 49. A tal proposito, è lecito trasferire dati personali verso un Paese terzo non adeguato "**per importanti motivi di interesse pubblico**", in deroga al divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto dell'Ue (art. 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

In merito ai requisiti per l'approvazione delle norme vincolanti d'impresa ed i contenuti obbligatori di tali norme, l'approvazione stessa deve avvenire esclusivamente attraverso il meccanismo di coerenza (artt. 63-65) – ovvero, è previsto in ogni caso l'intervento del Comitato Europeo per la protezione dei dati (art. 64, paragrafo 1, lettera d)).

12. REGOLE FONDAMENTALI PER LA CONFORMITÀ DI UN SITO WEB

Con le nuove disposizioni introdotte dal Regolamento (UE) 2016/679, in riferimento alla tutela della privacy dei consumatori, tutte le società che hanno un sito web e che elaborano le informazioni sensibili dei propri utenti devono adeguarsi in tal senso.

12.1 GDPR e Sito Web: diritto alla cancellazione dei dati personali

In conformità con quanto stabilito, i siti web devono dimostrare il possesso del fondamento giuridico per poter realizzare il trattamento dei dati. Tutte le procedure di trattamento vanno adoperate con il fine di proteggere i diritti dell'utente, a partire dalla richiesta cancellazione dei dati personali che può essere effettuata in qualsiasi momento.

Per facilitare la procedura di richiesta della cancellazione dei dati personali è necessario che venga creato un apposito database separato per il consenso degli utenti.

12.2 GDPR e Sito Web: registrazione dei Log

La conformità del GDPR per i nuovi siti richiede anche l'implementazione di un sistema di verifica dei dati dei visitatori, con possibilità di notifica immediata in caso di rischio di violazione dei dati personali. A tal proposito il Log Management rappresenta lo strumento efficace per far fronte a queste esigenze; in particolare, soddisfare disposizioni normative, contare su uno strumento di monitoraggio e controllo e garantire alti standard di sicurezza.

Se il file di log ha anche rilevanza giuridica e carattere probatorio, per poter essere attendibile ed inconfutabile come eventuale prova in giudizio, deve essere reso statico ed immodificabile e occorre garantirne l'autenticità dell'origine, l'integrità, la qualità e l'affidabilità. Per conferire tali caratteristiche, al file di log è consigliabile la sua conservazione digitale.

La soluzione più ottimale per garantire una idonea misura di sicurezza risulta perciò essere l'estrazione giornaliera del documento informatico (contenente i log da conservare), garantendone l'origine, per esempio apponendovi la firma digitale, in modo da assicurare la sua "cristallizzazione" giuridica.

12.3 GDPR e Sito Web: I diritti dell'interessato

Il GDPR si basa sui principi di trasparenza e correttezza in merito al trattamento di dati personali riconducibili a persone fisiche determinate o determinabili, pertanto vengono garantiti diversi diritti degli interessati, che effettuano accessi ai siti web, ed espressamente disciplinati agli artt. 12 e seguenti, e precisamente:

1) diritto di accesso (art. 15);
2) il diritto di rettifica (art. 16);
3) il diritto all'oblio (art. 17);
4) il diritto di limitazione al trattamento (art. 18);
5) il diritto alla portabilità dei dati (art.20);
6) il diritto di opposizione (art. 21).

12.4 GDPR e Sito Web: il diritto di essere informato

In ottemperanza della normativa del GDPR, nel rispetto dei diversi tipi di diritti dell'utente emerge soprattutto il diritto di essere informato.

Ogni comunicazione che richiama tale diritto devono essere visualizzati, nel sito web, in modo chiaro e facilmente comprensibile, anche per bambini o minorenni.

Gli amministratori dei siti devono inoltre effettuare una divisione tra due categorie, per distinguere dati ottenuti direttamente dagli utenti e dati secondari raccolti in base ad informazioni.

12.5 GDPR e Sito Web: la newsletter

Anche le opzioni di abbonamento alla newsletter e le preferenze di contatto costituiscono oggetto di disciplina al fine di allinearsi con le nuove disposizioni.

I moduli dovranno essere riadattati, con un passaggio dei messaggi sponsorizzati e delle newsletter da opt-out (il destinatario riceve la newsletter fino a quando non dichiara in modo esplicito di non voler ricevere messaggi dalla lista) ad opt-in (iscrizione in una lista e dunque consenso esplicito del destinatario a ricevere comunicazione per via mail). Lo stesso vale per "Termini di servizio – condizioni" ed anche per la Privacy Policy.

12.6 GDPR e Sito Web: la gestione dei dati personali

Una volta fornito il consenso e l'accettazione dell'informativa sulla privacy e delle condizioni d'uso, l'utente deve avere la possibilità di gestire i dati in modo semplice ed immediato. Un approccio consigliato è quello di creare una pagina del profilo utente, dove poter gestire autonomamente qualsiasi consenso sulla raccolta dati privati e qualsiasi invio di comunicazioni e newsletter.

In forma sintetica, è possibile elencare i passaggi principali con le azioni specifiche che è necessario seguire:

1) Realizzare una verifica di tutti i dati personali raccolti;
2) Aggiornare l'informativa sulla privacy;
3) Rendere affermativi gli avvisi dei cookies;
4) Creare semplici processi opt-in tali (a seconda del trattamento);
5) Rivedere la funzionalità di acquisizione dati;
6) Aggiornare le Privacy Policy per le e-mail;
7) Rendere immediata la possibilità di gestione/cancellazione dati;
8) Applicare un livello di crittografia sui dati presenti fisicamente sul disco e sulle informazioni nei database;
9) Controllare che tutti i moduli non siano "flaggati" di default. L'utente deve confermare l'invio delle informazioni;
10) Abilitare una procedura per agevolare l'eliminazione dei dati di un particolare utente;
11) Abilitare una procedura che garantisca la portabilità dei dati.

13. SANZIONI

Ai sensi dell'art. 83 del Regolamento (UE) 2016/679, viene definito un sistema sanzionatorio caratterizzato da diverse modalità, ovvero il richiamo, l'ammonizione, la sospensione dal trattamento dei dati e sanzioni pecuniarie fino a 20 milioni di euro oppure il 4% del fatturato totale annuale.

PARTE 2 – Sezione operativa

1 PRESENTAZIONE AZIENDA

Azienda	Società agricola semplice Belmonte di Mazzilli Rosa Anna
Attività svolta presso la sede operativa	Allevamento di pollame e vendita di uova
Sede legale	Via Pitagora n. 30 - 70033 Corato (BA)
Sede operativa	S.P. 231 SC Parco del Fornello - 70037 Ruvo di Puglia (BA)
Legale rappresentante	Amministratore: Sig.ra Mazzilli Rosa Anna
Titolare del Trattamento	Società agricola semplice Belmonte di Mazzilli Rosa Anna Via Pitagora n. 30 70033 Corato (BA)
Responsabile del trattamento	Sig.ra Mazzilli Rosa Anna
Responsabile della Protezione dei dati (RPD)	Non necessario e non nominato

2 ANALISI DEL CICLO PRODUTTIVO E DEI PROCESSI

La ditta ***"Società Agricola semplice Belmonte di Mazzilli Rosa Anna"*** svolge principalmente attività di allevamento a terra di galline e commercializzazione di uova presso vari punti vendita distribuiti tra Corato, Barletta e Ruvo di Puglia. Si prevede pertanto la vendita di uova sia all'ingrosso che al dettaglio. Lo scopo del presente paragrafo è quello di fornire una descrizione dettagliata del ciclo produttivo al fine di fornire un sopporto per la definizione dell'attività produttiva. In riferimento a quanto previsto dalla bibliografia di riferimento, è possibile fornire il flow chart indicato dalla bibliografia, tale riferimento è considerato quale punto di partenza per la contestualizzazione dello specifico ciclo produttivo.

Flow chart di riferimento

Cercando di contestuallizzare il più possibile il ciclo produttivo è possibile individuare le seguenti macro fasi di lavoro:

1. Pulizia e allevamento:

La pulizia dei locali di allevamento consiste nella asportazione di tutti i residui solidi e/o solido-polverosi dalle superfici dell'impianto, in un primo tempo per mezzo di attrezzi manuali quali scope e/o similari e successivamente mediante impiego di aria compressa. L'uso di aria compressa ha il duplice scopo di staccare le rimanenze di materiale organico dalle parti fisse dell'impianto e di convogliare le stesse e le altre particelle polverose verso una specifica zona del capannone dove ne risulta poi facilitata la rimozione. Il residuo solido così accumulato viene poi raccolto e condotto all'esterno dell'area di lavoro con sistemi manuali.

2. Lavaggio e disenfezione capannone e mangiatoie:

Terminata la fase di rimozione e smaltimento degli inquinanti di natura solida, viene realizzato il lavaggio di ambienti, attrezzature e pavimenti, facendo uso di idropulitrice. Terminata tale operazione si dà luogo alla rimozione degli eventuali residui di mangime dalla superficie delle mangiatoie. Terminata questa prima serie di operazioni, gli ambienti sono lasciati a riposo, dopo di che si procede alla disinfezione vera e propria di locali, impianti e attrezzature.

3. Scarico galline:

Concluse le fasi preparatorie dell'impianto, consistenti nelle operazioni di pulizia, lavaggio e disinfezione, si procede con l'immissione delle galline.

4. Allevamento a terra:

Le galline sono allevate all'interno di spazi aperti recintati. Le galline dispongono di molti "spazi in comune" in tutto l'edificio e possono muoversi liberamente. Vengono anche forniti loro nidi (con superficie "grattabile"), posatoi e lettiera sul suolo. Paragonati alle gabbie, questi sistemi permettono alle galline una maggiore libertà di muoversi, spiegare le ali e volare. La ditta dispone al contempo di un'area coperta per l'allevamento delle galline.

5. Raccolta e selezione delle uova:

La fase di raccolta e confezionamento delle uova consiste nell'attività giornaliera di recupero e confezionamento delle stesse. Nella struttura dell'impianto di allevamento è inserito un sistema di nastri trasportatori, idoneo alla raccolta automatica delle uova, le quali cadono per gravità sulla superficie del nastro sottostante le gabbie di allevamento. Giornalmente, il nastro viene azionato e le uova ivi presenti vengono così convogliate ad un macchinario adibito alla raccolta ed allo stoccaggio temporaneo di tale prodotto. Gli operatori addetti a questo macchinario realizzano dapprima una selezione manuale del prodotto, rimovendo le uova rotte e/o apparentemente sporche, quindi procedono al loro inserimento nelle apposite confezioni in cartone, normalmente della capacità di 30 uova cadauno. Le singole confezioni procedono poi mediante un ulteriore sistema a nastro trasportatore, sino al loro stoccaggio nell'imballaggio definitivo su pallets ai fini della spedizione.

6. Carico delle galline:

Trascorso un periodo di permanenza più o meno pari a circa 15 mesi, le galline non sono più produttive e vengono prelevate, inserite in gabbie da trasporto e caricate su automezzo per il conferimento alla macellazione. Le gabbie da trasporto sono di regola formate in materiale plastico e hanno capacità pari a 13-14 capi cadauna. Le gabbie possono essere movimentate per mezzo di carrelli manuali, poi caricate su automezzo per il trasporto al macello. Si riportano alcune immagini degli ambienti di lavoro:

Fig.1 – Area allevamento (esterna)

Fig. 2 – Area allevamento (interna)

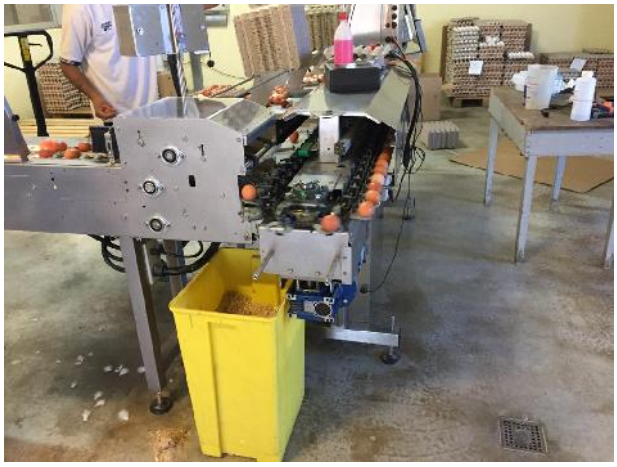


Fig. 3 – Selezionatrice uova

Occorre annoverare la presenza di uffici destinati alla gestione amministrativa, contabile ovvero la gestione dei clienti e dei fornitori nonché la gestione del personale, inoltre vi è un ufficio dedicato alle ricerche di mercato ed operazioni di marketing diretto.

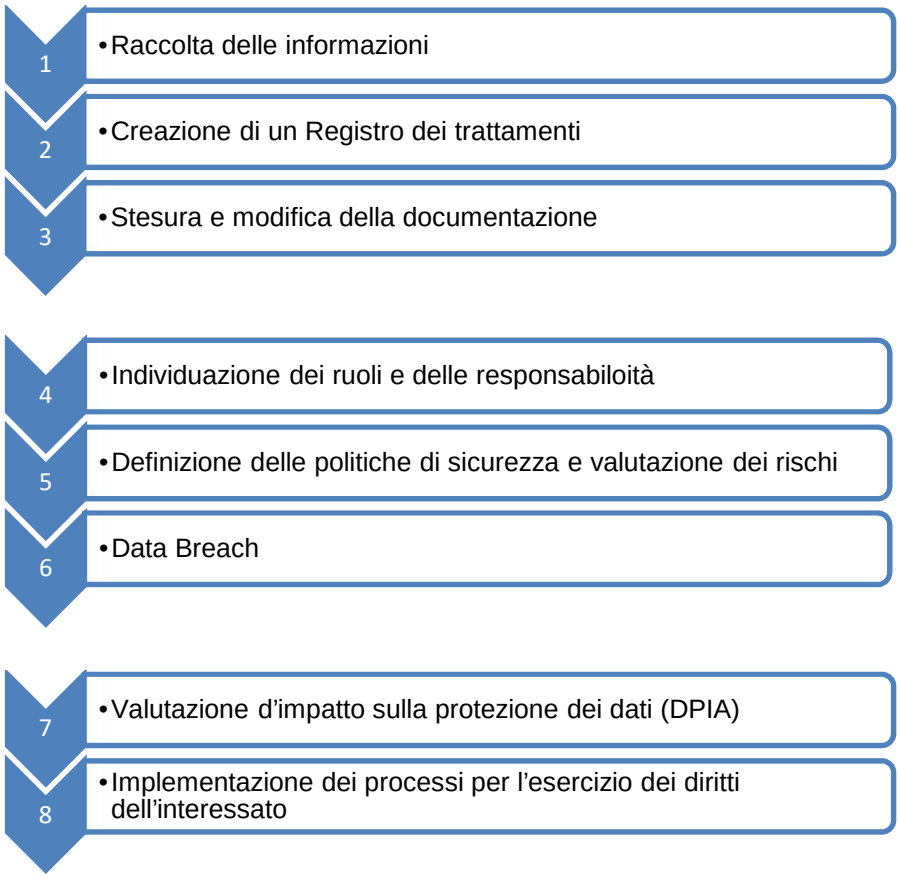
Tutte le aree aziendali sono tutelate mediante impianto di video sorveglianza posto in essere nel rispetto della normativa vigente nonché registrato mediante apposita istanza presso gli uffici della Direzione Territoriale del Lavoro di Bari.

Lo svolgimento dell'operatività aziendale richiede necessariamente l'acquisizione e gestione di dati, gli stessi sono principalmente annoverabili quali dati di natura amministrativa e contabile. Al contempo in ottemperanza a quanto previsto dal Reg. UE 2016/679 e D.Lgs 101/2018 si pone in essere il protocollo di gestione delle corrette prassi operative per l'acquisizione e gestione dei dati, verosimilmente anche dati personali che possono potenzialmente identificare in maniera univoca persone fisiche. In tal senso la gestione dei dati avviene anche mediante l'utilizzo di appositi strumenti informatici e secondo procedure informatizzate approvate dal responsabile IT (esterno), e pertanto in continuo monitoraggio e se necessario aggiornamento, le prassi operative nonché il processo di gestione mediante procedure informatizzate sarà oggetto di focus dedicato nello specifico paragrafo.

I processi operativi di acquisizione e gestione dei dati, nonché quelli maggiormente significativi possono essere riassunti nel seguente elenco:

1) Gestione delle risorse umane;
2) Gestione dei clienti;
3) Gestione dei fornitori;
4) Gestione delle attività mediante sito web, che svolge sia funzione di vetrina aziendale che di contatto con l'utenza;
5) Gestione dei profili aziendali su piattaforme social network;
6) Gestione newsletter e comunicazioni email (accountability relativamente agli account di posta aziendali);
7) Gestione impianto di videosorveglianza.

Al fine di poter meglio identificare i rischi connessi alla gestione dei dati acquisiti è possibile riportare un flow chart indicativo dello specifico profilo di rischio:



Si riporta a seguito del flow chart una rapida descrizione di ogni fase di lavoro precedentemente indicata

1) **RACCOLTA DELLE INFORMAZIONI**

Valutazione della "compliance", ovvero della conformità dei dati raccolti.

2) **CREAZIONE DEL REGISTRO DEI TRATTAMENTI**

Un Registro delle attività di trattamento svolte sotto la responsabilità del titolare del trattamento.

3) **STESURA/MODIFICA DELLA DOCUMENTAZIONE**

La documentazione deve necessariamente essere aggiornata e completa.

4) **INDIVIDUAZIONE DEI RUOLI E DELLE RESPONSABILITA'**

Definizioni dei ruoli e delle relative responsabilità di trattamento dei dati.

5) **DEFINIZIONE DELLE POLITICHE DI SICUREZZA E VALUTAZIONE DEI RISCHI**

Espressione ed applicazione del concetto di accountability, ovvero della "responsabilizzazione" del titolare e del responsabile del trattamento dei dati (ove nominato).

6) **DATA BREACH**

Adozione di tutte le procedure idonee ad individuare eventuali violazioni.

7) **VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI**

Valutazione degli aspetti relativi alla protezione dei dati, prima del loro trattamento.

8) **IMPLEMENTAZIONE DEI PROCESSI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO**

Procedure da adottare al fine di assicurare l'adozione di tutte le misure atte ad individuare eventuali violazioni.

3 TIPOLOGIA E TRATTAMENTO DATI

Il trattamento dei dati acquisiti viene effettuato mediante strumenti idonei a garantire la sicurezza e riservatezza dell'interessato a cui i dati in questione fanno riferimento.

I dati acquisiti vengono trattati, sfruttando anche processi automatizzati e/o di profilazione, in modo lecito e secondo principi di correttezza e trasparenza, registrati per scopi determinati, espliciti e legittimi e conservati mediante modalità che consentono l'identificazione dell'interessato. L'acquisizione dei dati avviene mediante l'espletamento dei seguenti processi:

1) gestione sito web: vetrina aziendale;
2) gestione richieste di informazioni, da social network, da parte del cliente mediante piattaforma dedicata;
3) gestione comunicazioni email;
4) gestione risorse umane;
5) gestione clienti;
6) gestione fornitori;
7) gestione videosorveglianza.

3.1 INFORMAZIONI RACCOLTE DAL SITO WEB (www.uovabelmonte.it)

La ditta ***"Società Agricola semplice Belmonte di Mazzilli Rosa Anna"*** utilizza il proprio sito vetrina per presentazione aziendale, nonché per la presentazione delle differenti tipologie di uova commercializzate. Al contempo non si prevede l'utilizzo di sito web al fine di effettuare acquisti diretti e transazioni online per la fornitura di specifici prodotti e/o servizi. Il sito web svolge la funzione di portale informativo sui prodotti commercializzati (a marchio proprio). Al contempo è prevista la funzione "contatti", che permette l'invio di specifiche richieste attraverso comunicazione email o contatto telefonico. Si specifica che il sito web non permette l'utilizzo di tools diretti di contatto. Pertanto il cliente può prendere visione dell'indirizzo della sede operativa, indirizzo email e numero telefonico.

Di seguito esposte le principali modalità con cui il sito raccoglie informazioni dagli utenti:

1) Mediante corrispondenza, durante l'utilizzo dei recapiti indicati (recapito telefonico ed e-mail);

Occorre pertanto che l'utente possa e debba aver preso visione delle privacy policy prima dell'avvio del processo di acquisizione e gestione dei dati.

3.1.1. FINALITÀ DEL TRATTAMENTO DEI DATI RACCOLTI

I dati personali raccolti possono essere utilizzati per una serie di finalità:

1) finalità connesse alla fornitura dei prodotti e servizi;
2) finalità legate allo sviluppo della statistica e dell'interazione con social network/piattaforme esterne;
3) finalità rivolte ad assicurare il trattamento legittimo del dato e necessarie ad assicurare all'utente un servizio che risponda esigenze e aspettative.

3.1.2 BASE GIURIDICA DEL TRATTAMENTO

Il trattamento dei dati personali mediante piattaforma da sito web viene effettuato sulla base di misure volte ad adempiere ad un obbligo legale con il consenso prestato dall'interessato, in ogni momento liberamente revocabile. Di seguito si riportano i principali casi di utilizzo dei dati personali dell'utente e le basi giuridiche su cui essi si fondano, per attività inerenti la piattaforma "contatti" da sito web.

ATTIVITA'	BASI GIURIDICHE
Gestione delle richieste dell'utente Trattamento dei dati per gestire le richieste inviate dall'utente attraverso sito web.	Legittimo interesse a offrire un buon servizio attraverso il sito web.
Ottimizzazione della fruibilità del sito Precompilazione di campi di dati sul sito web per ottimizzare e velocizzare l'esperienza online.	Legittimo interesse a ottimizzare, semplificare e velocizzare gli utilizzi del sito web.
Attività interne di ricerca e sviluppo Attività interne riguardanti la ricerca, lo sviluppo e l'analisi (sviluppo della statistica e dell'interazione con social network/piattaforme esterne).	Legittimo interesse a valutare e migliorare la performance dei servizi resi e gestire la conformità dei servizi.
Sicurezza della rete e delle informazioni Salvaguardia della sicurezza della rete di comunicazione e delle informazioni in essa contenute, così da consentire la tutela dei dati dell'utente da perdite o danneggiamenti, furti e accessi non autorizzati. Assicurare un'ubicazione razionale dei server.	Obbligo di legge per garantire la sicurezza della rete di comunicazione e delle informazioni in essa contenute.

3.1.3 PROTEZIONE DEI DATI

La protezione dei dati raccolti si realizza, mediante idonee misure di sicurezza, considerando la natura, l'oggetto, il contesto, le finalità del trattamento ed anche il rischio di probabilità e/o gravità di lesione dei diritti e delle libertà delle persone fisiche. Tutti i dati personali vengono trattati nel massimo rispetto della legge:

sottoposti ad aggiornamenti e conservazione in tempi strettamente necessari all'erogazione dei servizi e prodotti richiesti dall'interessato, secondo i tempi massimi previsti dalla legge. Il processo di trattamento si realizza in completa sicurezza in modo da impedire l'accesso a soggetti terzi. Al contempo vengono garantiti e mai tralasciati i diritti dell'interessato, di cui:

1) il diritto di accedere ai propri dati personali;
2) la possibilità di controllare l'esattezza dei dati che lo riguardano;
3) la rettifica e/o l'integrazione degli stessi;
4) il diritto alla cancellazione o la limitazione del trattamento od opporsi allo stesso;
5) la possibilità di revocare il consenso prestato anche per singole tipologie di trattamento, nonché garantire la portabilità dei dati personali raccolti.

Il sito web non offre la possibilità di acquisti on line ovvero di transazioni dirette su piattaforme online, al contempo si utilizzano sistemi blocco e sicurezza ("https"), ovvero protocolli di sicurezza che permettono di identificare l'utente (ad esempio Transport Layer Security (TLS) e il suo predecessore Secure Sockets Layer (SSL)). Quanto posto in essere è assimilabile all'acquisizione di dati inerenti principalmente clienti identificabili in soggetti giuridici (società e affini) e (a seconda delle richieste pervenute) in persone fisiche. Quanto esplicitato ha obiettivo di identificare i dati acquisiti in informazioni necessarie al conseguimento delle finalità descritte per fini di natura commerciale. I rapporti commerciali tra la ditta e i clienti si esplicano sul territorio nazionale. In tal modo l'acquisizione e gestione dei dati per finalità di natura commerciale, e qualora necessario dei dati personali, viene effettuata sul territorio nazionale italiano in accordo ed applicazione con quanto disciplinato dal Reg. UE 2016/679 e D.Lgs 101/2018. Pertanto non si procede con il trasferimento di dati verso paesi terzi, bensì è veritiero che si proceda con l'acquisizione di dati provenienti da soggetti economici ed operatori (assimilabili a clienti) provenienti da paesi terzi. Si specifica che in accordo con quanto disciplinato dalla normativa di riferimento il trasferimento di dati personali da paesi appartenenti all´UE verso Paesi "terzi" (non appartenenti all´UE o allo Spazio Economico Europeo) è vietato (articolo 25, comma 1, della Direttiva 95/46/CE), a meno che il Paese in questione non garantisce un livello di protezione "adeguato". In tal senso la Commissione Europea ha stabilito tale adeguatezza attraverso specifiche decisioni (di cui articolo 25, comma 6, della Direttiva 95/46/CE). In deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall´articolo 26, comma 1, della Direttiva 95/46 (consenso della persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, ecc.), nonché sulla base di strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46). La Commissione Europea può stabilire, che il livello di protezione offerto in un determinato Paese risulti adeguato (articolo 25, comma 6, della Direttiva 95/46/CE), e che pertanto è possibile trasferirvi dati personali. Le decisioni definite dalla Commissione Europea definiscono specifici accordi con i paesi di seguito elencati, mediante le decisioni della Commissione pubblicate in materia di adeguatezza di Paesi terzi. Di seguito i paesi terzi interessati e le relative decisioni e azioni intraprese dalla Commissione Europea, specificando che qualora si renda necessario il trasferimento di dati verso paesi terzi verranno poste in essere le indicazioni operative esplicitate nelle seguenti decisioni della Commissione Europea, di seguito:

- ✓ Andorra (2010/625/UE: Decisione della Commissione, del 19 ottobre 2010, ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali ad Andorra);
- ✓ Argentina (Decisione della Commissione conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina - 30 giugno 2003);
- ✓ Australia (Accordo Europa – Australia, PNR);
- ✓ Canada (2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act);
- ✓ Faer Øer (2010/146/: Decisione della Commissione, del 5 marzo 2010 , ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione fornita dalla legge delle Isole FaerØer sul trattamento dei dati personali);
- ✓ Guernsey (2003/821/CE: Decisione della Commissione, del 21 novembre 2003, sulla adeguata protezione dei dati personali in Guernsey);
- ✓ Isola di Man (Commission decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man);
- ✓ Israele (2011/61/EU: Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data);
- ✓ Jersey (2008/393/CE: Decisione della Commissione, dell' 8 maggio 2008 , ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali a Jersey);
- ✓ Nuova Zelanda (DECISIONE-DELLA-COMMISSIONE-2013-65-UE-Nuova-Zelanda);
- ✓ Svizzera (Decisione della Commissione riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE - 26 luglio 2000);
- ✓ Uruguay (2012/484/EU: Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data);
- ✓ USA: Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull´adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy. (Privacy Shield);
- ✓ USA (USA – PNR: Commissione - Decisione 14 maggio 2004 Customs and Border Protection);
- ✓ Decisione di esecuzione (UE) 2016/2295 della Commissione, del 16 dicembre 2016, che modifica le decisioni 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE e le decisioni di esecuzione 2012/484/UE, 2013/65/UE riguardanti l´adeguatezza della protezione dei dati personali da parte di taluni paesi, a norma dell´articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio;

Il processo di trattamento dei dati si realizza in completa sicurezza in modo da impedire l'accesso a soggetti terzi.

3.1.4 QUALI DATI PERSONALI SONO RACCOLTI

I dati personali che possono essere raccolti mediante sito web e successivo contatto email e/o telefonico includono:

1) Nome;
2) E-mail;
3) Oggetto;
4) Messaggio;
5) Indirizzo di posta elettronica.

Le citate informazioni verranno utilizzate per le relative finalità:

1) finalità connesse alla fornitura dei prodotti;
2) finalità legate allo sviluppo della statistica e dell'interazione con social network/piattaforme esterne;
3) finalità rivolte ad assicurare il trattamento legittimo del dato e necessarie ad assicurare all'utente un servizio che risponda esigenze e aspettative.

3.1.5 TERMINI DI CONSERVAZIONE DEI DATI PERSONALI DELL'UTENTE

La conservazione dei dati personali si realizza, nel rispetto degli obblighi di legge, per rispondere a richieste di chiarimenti/risoluzioni di eventuali controversie e tutelare i legittimi interessi.

3.1.6 SOGGETTI CON CUI CONDIVIDERE I DATI PERSONALI

I dati personali dell'utente possono essere condivisi con i seguenti soggetti:

1) Soggetti terzi che ne hanno necessità affinché si possano fornire i prodotti richiesti: a titolo esemplificativo si considerano gli incaricati coinvolti nell'organizzazione del sito (personale amministrativo, commerciale, marketing, legali, amministratori di sistema) ovvero soggetti esterni (come fornitori di servizi tecnici terzi, hosting provider, società informatiche, agenzie di comunicazione);
2) Laddove esista l'obbligo di comunicare o condividere i dati personali dell'utente per ottemperare a un obbligo di legge, per darvi applicazione o per indagare, con gli enti di polizia giudiziaria preposti, su violazioni vere o presunte.

3.1.7 DIRITTI DELL'INTERESSATO

L'interessato ha il diritto di chiedere in qualsiasi momento:

1) L'accesso ai dati personali, (e/o una copia di tali Dati Personali), nonché ulteriori informazioni sui trattamenti in corso su di essi;
2) La rettifica o l'aggiornamento dei dati personali trattati, laddove fossero incompleti o non aggiornati;
3) La cancellazione dei dati personali dai database, laddove ritenesse il trattamento non necessario o illegittimo;
4) La limitazione del trattamento dei dati personali, laddove ritenesse che questi non siano corretti, necessari o siano illegittimamente trattati, o laddove si fosse opposto al loro trattamento;
5) Di esercitare il suo diritto alla portabilità dei dati, ossia di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico una copia dei dati personali forniti che lo riguardano, o di richiederne la trasmissione ad un altro Titolare;
6) Di opporsi al trattamento dei dati personali;
7) Di revocare il suo consenso prestato per le finalità distinte da analisi statistiche e di marketing diretto.

Per consentire un più celere riscontro delle richieste formulate nell'esercizio dei suddetti diritti, le stesse potranno essere rivolte inviando anche copia di un documento di identità, all'indirizzo postale della sede legale o all'indirizzo mail: info@uovabelmonte.it.

3.1.8 TUTELA DEI MINORI

Al fine di garantire la tutela dei minori, i servizi resi dalla ditta che possano determinare il porre in essere di potenziali obbligazioni contrattuali, sono riservati a soggetti giuridicamente "abilitati" nella misura in cui sulla base della normativa di riferimento, vengono rispettati i limiti, le modalità e i criteri di identificazione di soggetti "minori" e "non", nonché tutela di questi ultimi. In attuazione dell'art. 8, paragrafo 1, del Regolamento (UE) 2016/679, il minore che abbia compiuto i sedici anni può esprimere il consenso al trattamento dei propri dati personali. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a sedici anni, fondato sull'art. 6, paragrafo 1, lettera a), del Regolamento (UE) 2016/679, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale (Art. 2-quinquies). In ottemperanza a quanto riportato in merito alla tutela dei minori, occorre specificare che il D.Lgs 101/2018 in attuazione di quanto già espresso dal Regolamento UE 2016/679 ha di fatto abbassato il limite anagrafico ad anni quattordici per richiedere per minori di età inferiore il consenso di chi ne esercita la responsabilità genitoriale.

3.1.9 Cookies policy del sito web "www.uovabelmonte.it"

Cos'è un cookie e a cosa serve? Un cookie è un file di dimensioni ridotte che un sito invia al browser e salva sul computer dell'utente quando visita un sito internet come www.uovabelmonte.it. I cookies vengono

utilizzati per far funzionare il sito web o per migliorare le prestazioni, ma anche per fornire informazioni ai proprietari del sito stesso. Quali e quanti tipi di cookie un sito può utilizzare e a quale scopo? Esistono differenti tipologie di cookies tutti atti a garantire la corretta funzionalità di un sito web, ad esempio:

Cookies di navigazione: I cookies di navigazione permettono al sito web di funzionare correttamente e permettono di visualizzare i contenuti nella lingua dell'utente e per il suo mercato fin dal primo accesso. Sono in grado di riconoscere da quale Paese l'utente si sta connettendo e fanno in modo che, ogni volta che visiterà il sito, sarà automaticamente indirizzato alla versione del sito per il suo paese. Questo tipo di cookie permette di cercare un account, effettuare un login e gestire le informazioni rilasciate dall'utente. Se l'utente è già registrato, grazie ai cookie il sito potrà riconoscerlo come tale quando accederà ai servizi offerti agli utenti registrati. Questi cookie sono utili al buon funzionamento del sito.

Cookies funzionali: I cookies funzionali permettono al sito di riconoscere l'utente in base alla sua richiesta, ogni volta che accede al sito, cliccando ad esempio sul tasto "riconoscimi ogni volta" – se presente – in modo da non dover inserire nuovamente i suoi dati tutte le volte che visita il sito web. Questi cookie non sono necessari al funzionamento del sito web, ma ne migliorano la navigazione e la fruizione.

Cookies analitici: I cookies analitici sono utilizzati per esempio da Google Analytics per elaborare analisi statistiche sulle modalità di navigazione degli utenti sul sito, attraverso i computer o le applicazioni mobile, sul numero di pagine visitate o il numero di click effettuati su una pagina durante la navigazione di un sito. Il sito web della ditta "**Società Agricola Semplice Belmonte di Mazzilli Rosa Anna**" tratta i risultati di queste analisi in forma anonima ed esclusivamente per finalità analitiche solo se il fornitore dei servizi utilizza i cookie in connessione al browser installato sul suo computer su altri dispositivi utilizzati per navigare sul nostro sito.

Cookie di terze parti per marketing/retargeting: Questi cookie sono utilizzati da società di fiducia che permettono all'utente di visualizzare banner pubblicitari su altri siti affiliati, mostrandogli gli ultimi prodotti guardati sul sito web, specie se si tratta di e-commerce. Mentre l'utente naviga all'interno del sito, questi cookie sono utilizzati per mostrargli i prodotti che potrebbero interessargli o simili a quelli che ha guardato in precedenza, basandosi sulla cronologia di navigazione. L'uso di questi cookie normalmente non implica il trattamento di dati personali, ma può permettere la connessione al computer dell'utente o ad altri dispositivi e rintracciare i dati salvati: questi cookie si connettono al browser installato sul computer o su altri dispositivi dell'utente durante la navigazione sul sito.

Quali cookie utilizza il sito www.uovabelmonte.it dei cookie appena descritti, utilizza esclusivamente quelli di tipo analitico elencati qui di seguito:

Tipo di cookie e proprietario	Nome tecnico dei cookies	Tempo di persistenza	Funzionamento e finalità
Google Maps			
Google.com third-party Tracciamento	SSID	2 anni	Cookie utilizzato da Google Maps per tenere traccia del comportamento del visitatore. http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	SIDCC	3 mesi	Cookie utilizzato da Google Maps per tenere traccia del comportamento del visitatore. http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	SID	2 anni	Cookie utilizzato da Google Maps per tenere traccia del comportamento del visitatore. http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	1P_JAR	1 mese	Memorizza le preferenze e le informazioni dell'utente ogni volta che visita pagine web contenenti mappe geografiche di Google Maps. http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	APISID	2 anni	Cookie utilizzato da Google Maps per tenere traccia del comportamento del visitatore. http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	HSID	2 anni	Cookie utilizzato da Google Maps per tenere traccia del comportamento del visitatore. http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	NID	6 mesi	Cookie utilizzato da Google Maps per tenere traccia del comportamento del visitatore. http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	OTZ	1 mese	Cookie utilizzato da Google Maps per tenere traccia del comportamento del visitatore. http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	SAPISID	2 anni	Cookie utilizzato da Google Maps per tenere traccia del comportamento del visitatore. http://www.google.com/policies/privacy/
Google Analytics			
Google.com third-party Tracciamento	_ga	2 anni	Tracciano il numero e la tipologia di visite degli utenti per scopi statistici. Nello specifico usati per distinguere fra loro gli utenti http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	_gid	24 ore	Tracciano il numero e la tipologia di visite degli utenti per scopi statistici. Nello specifico usati per distinguere fra loro gli utenti http://www.google.com/policies/privacy/
Google.com third-party Tracciamento	_gat	1 minuto	Tracciano il numero e la tipologia di visite degli utenti per scopi statistici. Nello specifico usato per modificare la frequenza delle richieste. http://www.google.com/policies/privacy/

3.2 INFORMAZIONI RACCOLTE DA SOCIAL NETWORK

I social network (Facebook) svolgono la funzione di portali informativi sui prodotti forniti dalla ditta, servizi, approfondimenti. Le piattaforme definibili "social" utilizzate dalla ditta mediante la creazione di account ai quali vengono associate delle pagine dedicate sono, ad oggi, uno ovvero: Facebook. Tale canale opera mediante l'applicazione di policy privacy proprie ai quali l'utente accede e ne prende visione con accettazione. In tal senso la gestione dei dati potenzialmente acquisibili e processabili avviene direttamente dalle piattaforme e l'utente, in tal caso la ***"Società Agricola semplice Belmonte di Mazzilli Rosa Anna"*** (di seguito la ditta), ne usufruisce nelle modalità e per gli scopi esplicitati nella presente sezione. I contenuti riportati sono da intendersi quale implementazione delle policy privacy applicate dalle piattaforme social network verso le quali la ditta detiene un proprio account utilizzato solo ed esclusivamente per la presentazione dei propri prodotti e per le finalità esplicitate. In tal senso la ditta, quale soggetto giuridico dotato di un proprio organismo di gestione della privacy in accordo ed ai sensi del Reg. UE 2016/679 e D.Lgs 101/2018, viene sollevata da eventuali azioni poste in essere dai gestori delle piattaforme social network non conformi alla disciplina di riferimento e che possano potenzialmente ledere la libertà delle persone fisiche. Si riportano pertanto i riferimenti, consultabili in ogni momento e in continuo aggiornamento, in merito alle policy privacy applicate dalle piattaforme social network menzionate:

Facebook: https://it-it.facebook.com/privacy/explanation

3.2.1. FINALITÀ DEL TRATTAMENTO DEI DATI RACCOLTI

I dati personali raccolti possono essere utilizzati per una serie di finalità:

1) finalità connesse alla presentazione dei prodotti, dell'azienda e delle attività svolte;
2) finalità rivolte ad assicurare il trattamento legittimo del dato e necessarie ad assicurare all'utente un servizio che risponda esigenze e aspettative.

3.2.2 BASE GIURIDICA DEL TRATTAMENTO

Il trattamento dei dati personali effettuato mediante piattaforme di social network viene effettuato sulla base di misure volte ad adempiere ad un obbligo legale con il consenso prestato dall'interessato, in ogni momento liberamente revocabile. Di seguito si riportano i principali casi di utilizzo dei dati personali dell'utente e le basi giuridiche su cui essi si fondano, per attività inerenti le piattaforme da social network.

ATTIVITÀ	BASI GIURIDICHE
Gestione delle richieste dell'utente Trattamento dei dati per gestire le richieste inviate dall'utente attraverso social network.	Legittimo interesse a offrire un buon servizio attraverso il social network.

Sicurezza della rete e delle informazioni Salvaguardia della sicurezza della rete di comunicazione e delle informazioni in essa contenute, così da consentire la tutela dei dati dell'utente da perdite o danneggiamenti, furti e accessi non autorizzati. Assicurare un'ubicazione razionale dei server.	Obbligo di legge per garantire la sicurezza della rete di comunicazione e delle informazioni in essa contenute.

3.2.3 PROTEZIONE DEI DATI

La protezione dei dati raccolti si realizza, mediante idonee misure di sicurezza, considerando la natura, l'oggetto, il contesto, le finalità del trattamento ed anche il rischio di probabilità e/o gravità di lesione dei diritti e delle libertà delle persone fisiche.

Tutti i dati personali vengono trattati nel massimo rispetto della legge: sottoposti ad aggiornamenti e conservazione in tempi strettamente necessari alla fornitura dei prodotti richiesti dall'interessato, secondo i tempi massimi previsti dalla legge.

Il processo di trattamento si realizza in completa sicurezza in modo da impedire l'accesso a soggetti terzi; al contempo vengono garantiti e mai tralasciati i diritti dell'interessato, di cui:

1) il diritto di accedere ai propri dati personali;
2) la possibilità di controllare l'esattezza dei dati che lo riguardano;
3) la rettifica e/o l'integrazione degli stessi;
4) il diritto alla cancellazione o la limitazione del trattamento od opporsi allo stesso;
5) la possibilità di revocare il consenso prestato anche per singole tipologie di trattamento, nonché garantire la portabilità dei dati personali raccolti.

3.2.4 QUALI DATI PERSONALI SONO RACCOLTI

I dati personali raccolti mediante social network nella sezione "CONTATTI" includono:

1) Nome o nickname;
2) Recapiti telefonici e email;
3) Corpo del Messaggio.

Le citate informazioni verranno utilizzate per le relative finalità:

- ✓ finalità connesse alla fornitura dei prodotti, dell'azienda e delle attività svolte;
- ✓ finalità rivolte ad assicurare il trattamento legittimo del dato e necessarie ad assicurare all'utente un servizio che risponda esigenze e aspettative.

3.2.5 TERMINI DI CONSERVAZIONE DEI DATI PERSONALI DELL'UTENTE

La conservazione dei dati personali si realizza, nel rispetto degli obblighi di legge, per rispondere a richieste di chiarimenti/risoluzioni di eventuali controversie e tutelare i legittimi interessi.

3.2.6 SOGGETTI CON CUI CONDIVIDERE I DATI PERSONALI

I dati personali dell'utente possono essere condivisi con i seguenti soggetti:

1) Soggetti terzi che ne hanno necessità affinché si possano fornire i prodotti richiesti: a titolo esemplificativo si considerano gli incaricati coinvolti nell'organizzazione del social network ovvero soggetti esterni (come fornitori di servizi tecnici terzi, hosting provider, società informatiche, agenzie di comunicazione);
2) Laddove esista l'obbligo di comunicare o condividere i dati personali dell'utente per ottemperare a un obbligo di legge, per darvi applicazione o per indagare, con gli enti di polizia giudiziaria preposti, su violazioni vere o presunte.

3.2.7 DIRITTI DELL'INTERESSATO

L'interessato ha il diritto di chiedere in qualsiasi momento:

1) L'accesso ai dati personali, (e/o una copia di tali Dati Personali), nonché ulteriori informazioni sui trattamenti in corso su di essi;
2) La rettifica o l'aggiornamento dei dati personali trattati, laddove fossero incompleti o non aggiornati;
3) La cancellazione dei dati personali dai database, laddove ritenesse il trattamento non necessario o illegittimo;
4) La limitazione del trattamento dei dati personali, laddove ritenesse che questi non siano corretti, necessari o siano illegittimamente trattati, o laddove si fosse opposto al loro trattamento;
5) Di esercitare il suo diritto alla portabilità dei dati, ossia di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico una copia dei dati personali forniti che lo riguardano, o di richiederne la trasmissione ad un altro Titolare;
6) Di opporsi al trattamento dei dati personali;
7) Di revocare il suo consenso prestato per le finalità distinte da analisi statistiche e di marketing diretto.

Per consentire un più celere riscontro delle richieste formulate nell'esercizio dei suddetti diritti, le stesse potranno essere rivolte inviando anche copia di un documento di identità, all'indirizzo postale della sede legale o all'indirizzo mail: info@uovabelmonte.it.

3.2.8 TUTELA DEI MINORI

Al fine di garantire la tutela dei minori, i servizi resi dalla ditta che possano determinare il porre in essere di potenziali obbligazioni contrattuali, sono riservati a soggetti giuridicamente "abilitati" nella misura in cui sulla base della normativa di riferimento, vengono rispettati i limiti, le modalità e i criteri di identificazione di soggetti "minori" e "non", nonché tutela di questi ultimi. In attuazione dell'art. 8, paragrafo 1, del Regolamento (UE) 2016/679, il minore che abbia compiuto i sedici anni può esprimere il consenso al trattamento dei propri dati personali. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a sedici anni, fondato sull'art. 6, paragrafo 1, lettera a), del Regolamento (UE) 2016/679, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale (Art. 2-quinquies). In ottemperanza a quanto riportato in merito alla tutela dei minori, occorre specificare che il D.Lgs 101/2018 in attuazione di quanto già espresso dal Regolamento UE 2016/679 ha di fatto abbassato il limite anagrafico ad anni quattordici per richiedere per minori di età inferiore il consenso di chi ne esercita la responsabilità genitoriale.

3.3 GESTIONE RISORSE UMANE

Il processo prevede il trattamento dei dati relativamente ai dipendenti ("lavoratori") operanti presso la sede operativa della ditta, e non di soggetti terzi, non legati da vincolo lavorativo di subordinazione direttamente correlabile alla direzione aziendale (ovvero "datore di lavoro" secondo definizione ed accezione, come da D.Lgs 81/08 e s.m.i.), che a vario titolo operano presso la sede aziendale. Al contempo però quale applicazione di procedure operative condivise la ditta fornirà anche ai propri collaboratori informativa in merito alla gestione dei dati degli stessi.

3.3.1 FINALITÀ DEL TRATTAMENTO DEI DATI RACCOLTI DAI DIPENDENTI

I dati personali raccolti possono essere utilizzati per una serie di finalità relative la gestione delle attività amministrative:

1) definizione del rapporto di lavoro subordinato;
2) elaborazione cartelle per la retribuzione;
3) espletamento di tutte le pratiche previste dalle normative vigenti in materia di Sicurezza sul Lavoro, Privacy, tutela dei lavoratori afferente l'installazione e utilizzo di impianto di videosorveglianza;
4) adempimento degli obblighi legali e contrattuali connessi al rapporto di lavoro.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯Acconsento ◯Non acconsento

3.3.2 BASE GIURIDICA DEL TRATTAMENTO

Il trattamento dei dati personali viene effettuato sulla base giuridica dell'esecuzione di misure contrattuali, ovvero per adempiere ad un obbligo legale con il consenso prestato dall'interessato, in ogni momento liberamente revocabile. Nel registro dei trattamenti, redatto a cura del titolare del trattamento, vi è riportata apposita sezione nella quale per ogni processo gestito si dovrà indicare ai sensi dell'art. 6 (base giuridica su cui si fonda il trattamento) ed al contempo art. 9 (base giuridica per il trattamento di particolari categorie di dati) la base giuridica sulla quale si basa il trattamento dei dati raccolti. In dettaglio si segua la tabella riportata.

ATTIVITÀ	BASE GIURIDICA (art.6)	BASE GIURIDCA (art.9)
Attività di gestione delle risorse umane	Consenso dell'interessato Esecuzione di un contratto Obbligo legale Legittimo interesse del Titolare	Consenso dell'interessato Esercizio obblighi in materia di diritto del lavoro Esercizio obblighi in materia di protezione sociale Esistenza del segreto professionale

3.3.3 PROTEZIONE DEI DATI E TRASFERIMENTO DEI DATI PERSONALI

La protezione dei dati raccolti si realizza, mediante idonee misure di sicurezza, considerando la natura, l'oggetto, il contesto, le finalità del trattamento ed anche il rischio di probabilità e/o gravità di lesione dei diritti e delle libertà delle persone fisiche. Tutti i dati personali vengono trattati nel massimo rispetto della legge, sottoposti ad aggiornamenti e conservazione in tempi strettamente necessari, secondo i tempi massimi previsti dalla legge. Il processo di trattamento si realizza in completa sicurezza in modo da impedire l'accesso a soggetti terzi; al contempo vengono garantiti e mai tralasciati i diritti dell'interessato, di cui:

1) Diritto di accesso (ART. 15)
2) Diritto di rettifica (ART. 16)
3) Diritto di cancellazione (diritto all'oblio) (ART. 17)
4) Diritto di limitazione del trattamento (ART. 18)
5) Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (ART. 19)
6) Diritto alla portabilità dei dati (ART. 20)
7) Diritto di opposizione (ART. 21)

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯Acconsento ◯Non acconsento

3.3.4 QUALI DATI SONO RACCOLTI

I dati personali raccolti possono includere riferimenti a:

1) Nome e Cognome;
2) Sesso;
3) Data e Luogo di nascita;
4) Cod. Fiscale;
5) Domicilio;
6) Comune di domicilio;
7) Livello istruzione.

I dati richiesti risultato congrui a quanto previsto dalla normativa di riferimento in materia di tutela del rapporto di lavoro. Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯ **Acconsento** ◯**Non acconsento**

3.3.5 TERMINI DI CONSERVAZIONE DEI DATI PERSONALI DELL'UTENTE

La conservazione dei dati personali si realizza nelle modalità e tempistiche previste nel rispetto degli obblighi di legge, nonché al contempo per la risoluzione di eventuali controversie e tutelare i legittimi interessi del titolare del trattamento e dell'interessato.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.3.6 SOGGETTI CON CUI CONDIVIDERE I DATI PERSONALI

I dati personali dell'interessato possono essere condivisi con i seguenti soggetti:

1) Soggetti terzi che ne hanno necessità secondo obblighi di legge e/o secondo richieste esplicite (a titolo esemplificativo si considerano INPS, INAIL, Direzione provinciale del lavoro, Commercialista e Consulente del lavoro);
2) Laddove esista l'obbligo di comunicare o condividere i dati personali dell'utente per ottemperare a un obbligo di legge, per darvi applicazione o per indagare, con gli enti di polizia giudiziaria preposti, su violazioni vere o presunte.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la pressi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.3.7 DIRITTI DELL'INTERESSATO

L'interessato ha il diritto di chiedere in qualsiasi momento:

1) L'accesso ai dati personali, (e/o una copia di tali Dati Personali), nonché ulteriori informazioni sui trattamenti in corso su di essi;
2) La rettifica o l'aggiornamento dei dati personali trattati, laddove fossero incompleti o non aggiornati;
3) La cancellazione dei dati personali dai database, laddove ritenesse il trattamento non necessario o illegittimo;
4) La limitazione del trattamento dei dati personali, laddove ritenesse che questi non siano corretti, necessari o siano illegittimamente trattati, o laddove si fosse opposto al loro trattamento;
5) La notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;
6) La portabilità dei dati, ossia di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico una copia dei dati personali forniti che lo riguardano, o di richiederne la trasmissione ad un altro Titolare;
7) Di opporsi al trattamento dei dati personali.

Per consentire un più celere riscontro delle richieste formulate nell'esercizio dei suddetti diritti, le stesse potranno essere rivolte inviando anche copia di un documento di identità, all'indirizzo postale della sede legale o all'indirizzo mail: info@uovabelmonte.it.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.3.8 TUTELA DEI MINORI

Al fine di garantire la tutela dei minori la fornitura di rapporto di lavoro è riservata a soggetti giuridicamente in grado, sulla base della normativa di riferimento, di concludere obbligazioni contrattuali e nei limiti e modalità stabiliti dalla normativa di riferimento. In attuazione dell'art. 8, paragrafo 1, del Regolamento (UE) 2016/679, il minore che ha compiuto i sedici anni può esprimere il consenso al trattamento dei propri dati personali. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a sedici anni, fondato sull'art. 6, paragrafo 1, lettera a), del Regolamento (UE) 2016/679, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale. (Art. 2-quinquies - Consenso del minore in relazione ai servizi della

società dell'informazione). In ottemperanza a quanto riportato in merito alla tutela dei minori, occorre specificare che il D.Lgs 101/2018 in attuazione di quanto già espresso dal Regolamento UE 2016/679 ha di fatto abbassato il limite anagrafico ad anni quattordici per richiedere per minori di età inferiore il consenso di chi ne esercita la responsabilità genitoriale.

◯**Acconsento** ◯**Non acconsento**

3.4 GESTIONE CLIENTI

Il processo prevede il trattamento dei dati relativi alla gestione dei clienti, ovvero fruitori dei prodotti e dei servizi offerti dalla ditta, l'identificazione dei clienti avviene anche mediante strumenti informatici. In tal caso la gestione dei clienti e delle relative richieste di prodotti e/o servizi avviene attraverso piattaforme dedicate e riconducibili alle procedure di governo e gestione secondo quanto esplicitato e disponibile su sito web aziendale (www.uovabelmonte.it) e su canali "vetrina" su piattaforme social network, di cui anche in tal caso è possibile la consultazione delle policy su sito web.

3.4.1 FINALITÀ DEL TRATTAMENTO DEI DATI RACCOLTI DAI CLIENTI

I dati personali raccolti possono essere utilizzati per una serie di finalità rivolte alla fornitura di prodotti, servizi, ovvero per rispondere a diverse esigenze riscontrabili e di seguito indicate:

1) archiviazione e gestione dei dati inerenti clienti;
2) conformità degli obblighi e degli adempimenti (amministrativi, fiscali, contabili, etc.) disposti dalla legislazione vigente.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.4.2 BASE GIURIDICA DEL TRATTAMENTO

Il trattamento dei dati viene effettuato sulla base giuridica dell'esecuzione di misure contrattuali adottate, ovvero per adempiere ad un obbligo legale con il consenso prestato dall'interessato, in ogni momento liberamente revocabile.

Nel registro dei trattamenti, redatto a cura del titolare del trattamento, vi è riportata apposita sezione nella quale per ogni processo gestito si dovrà indicare ai sensi dell'art. 6 (base giuridica su cui si fonda il

trattamento) ed al contempo art. 9 (base giuridica per il trattamento di particolari categorie di dati) la base giuridica sulla quale si basa il trattamento dei dati raccolti.

In dettaglio si segua la tabella riportata:

ATTIVITÀ	BASE GIURIDICA (art.6)	BASE GIURIDCA (art.9)
Gestione clienti	Consenso dell'interessato Esecuzione di un contratto Obbligo legale Legittimo interesse del Titolare	Consenso dell'interessato

3.4.3 PROTEZIONE DEI DATI E TRASFERIMENTO DEI DATI PERSONALI

La protezione dei dati raccolti si realizza, mediante idonee misure di sicurezza, considerando la natura, l'oggetto, il contesto, le finalità del trattamento ed anche il rischio di probabilità e/o gravità di lesione dei diritti e delle libertà delle persone fisiche. Tutti i dati personali vengono trattati nel massimo rispetto della legge: sottoposti ad aggiornamenti e conservazione in tempi strettamente necessari all'erogazione dei servizi e prodotti richiesti dall'interessato, secondo i tempi massimi previsti dalla legge. Il processo di trattamento si realizza in completa sicurezza in modo da impedire l'accesso a soggetti terzi. Al contempo vengono garantiti e mai tralasciati i diritti dell'interessato, di cui:

1) il diritto di accedere ai propri dati personali;
2) la possibilità di controllare l'esattezza dei dati che lo riguardano;
3) la rettifica e/o l'integrazione degli stessi;
4) il diritto alla cancellazione o la limitazione del trattamento od opporsi allo stesso;
5) la possibilità di revocare il consenso prestato anche per singole tipologie di trattamento, nonché garantire la portabilità dei dati personali raccolti.

Quanto posto in essere è assimilabile all'acquisizione di dati inerenti principalmente clienti identificabili in soggetti giuridici (società e affini) e (a seconda delle richieste pervenute) in persone fisiche. Quanto esplicitato ha obiettivo di identificare i dati acquisiti in informazioni necessarie al conseguimento delle finalità descritte per fini di natura commerciale. I rapporti commerciali tra la ditta e i clienti si esplicano sul territorio nazionale. In tal modo l'acquisizione e gestione dei dati per finalità di natura commerciale, e qualora necessario dei dati personali, viene effettuata sul territorio nazionale italiano in accordo ed applicazione con quanto disciplinato dal Reg. UE 2016/679 e D.Lgs 101/2018. Pertanto non si procede con il trasferimento di dati verso paesi terzi, bensì è veritiero che si proceda con l'acquisizione di dati provenienti da soggetti economici ed operatori (assimilabili a clienti) provenienti da paesi terzi. Si specifica che in accordo con quanto disciplinato dalla normativa di riferimento il trasferimento di dati personali da paesi appartenenti all´UE verso Paesi "terzi" (non appartenenti all´UE o allo Spazio Economico Europeo) è vietato (articolo 25, comma 1, della Direttiva 95/46/CE), a meno che il Paese in questione non garantisce un livello di protezione

"adeguato". In tal senso la Commissione Europea ha stabilito tale adeguatezza attraverso specifiche decisioni (di cui articolo 25, comma 6, della Direttiva 95/46/CE). In deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall´articolo 26, comma 1, della Direttiva 95/46 (consenso della persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, ecc.), nonché sulla base di strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46). La Commissione Europea può stabilire, che il livello di protezione offerto in un determinato Paese risulti adeguato (articolo 25, comma 6, della Direttiva 95/46/CE), e che pertanto è possibile trasferirvi dati personali. Le decisioni definite dalla Commissione Europea definiscono specifici accordi con i paesi di seguito elencati, mediante le decisioni della Commissione pubblicate in materia di adeguatezza di Paesi terzi. Di seguito i paesi terzi interessati e le relative decisioni e azioni intraprese dalla Commissione Europea, specificando che qualora si renda necessario il trasferimento di dati verso paesi terzi verranno poste in essere le indicazioni operative esplicitate nelle seguenti decisioni della Commissione Europea, di seguito:

- ✓ Andorra (2010/625/UE: Decisione della Commissione, del 19 ottobre 2010, ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali ad Andorra);
- ✓ Argentina (Decisione della Commissione conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina - 30 giugno 2003);
- ✓ Australia (Accordo Europa – Australia, PNR);
- ✓ Canada (2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act);
- ✓ Faer Øer (2010/146/: Decisione della Commissione, del 5 marzo 2010 , ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione fornita dalla legge delle Isole FaerØer sul trattamento dei dati personali);
- ✓ Guernsey (2003/821/CE: Decisione della Commissione, del 21 novembre 2003, sulla adeguata protezione dei dati personali in Guernsey);
- ✓ Isola di Man (Commission decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man);
- ✓ Israele (2011/61/EU: Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data);
- ✓ Jersey (2008/393/CE: Decisione della Commissione, dell' 8 maggio 2008 , ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali a Jersey);
- ✓ Nuova Zelanda (DECISIONE-DELLA-COMMISSIONE-2013-65-UE-Nuova-Zelanda);
- ✓ Svizzera (Decisione della Commissione riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE - 26 luglio 2000);

- ✓ Uruguay (2012/484/EU: Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data);
- ✓ USA: Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull´adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy. (Privacy Shield);
- ✓ USA (USA – PNR: Commissione - Decisione 14 maggio 2004 Customs and Border Protection);
- ✓ Decisione di esecuzione (UE) 2016/2295 della Commissione, del 16 dicembre 2016, che modifica le decisioni 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE e le decisioni di esecuzione 2012/484/UE, 2013/65/UE riguardanti l´adeguatezza della protezione dei dati personali da parte di taluni paesi, a norma dell´articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio;

Il processo di trattamento dei dati si realizza in completa sicurezza in modo da impedire l'accesso a soggetti terzi.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.4.4 QUALI DATI SONO RACCOLTI

I dati raccolti possono includere riferimenti a:

1) Dati anagrafici (se necessario in riferimento a persone fisiche): Nome, Cognome, Data e Luogo di nascita, Residenza;
2) Ragione sociale (persone giuridiche);
3) Cod. Fiscale e/o Partita IVA (engl. Version: TIN (or EU TIN), VAT Identification Number, and/or equivalent fiscal number for European and non-European country);
4) Recapito telefonico;
5) Recapito e-mail.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯ **Acconsento** ◯**Non acconsento**

3.4.5 TERMINI DI CONSERVAZIONE DEI DATI PERSONALI DELL'UTENTE

La conservazione dei personali si realizza, nel rispetto degli obblighi di legge, per rispondere a richieste di chiarimenti/risoluzioni di eventuali controversie e tutelare i legittimi interessi del titolare del trattamento e dell'interessato.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la pressi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.4.6 SOGGETTI CON CUI CONDIVIDERE I DATI PERSONALI

I dati acquisiti potranno essere comunicati ai seguenti soggetti:

1) Soggetti terzi che ne hanno necessità secondo obblighi di legge e/o secondo richieste esplicite;
2) Laddove esista l'obbligo di comunicare o condividere i dati personali dell'utente per ottemperare a un obbligo di legge, per darvi applicazione o per indagare, con gli enti di polizia giudiziaria preposti, su violazioni vere o presunte.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.4.7 DIRITTI DELL'INTERESSATO

L'interessato ha il diritto di chiedere in qualsiasi momento:

1) L'accesso ai dati personali, (e/o una copia di tali Dati Personali), nonché ulteriori informazioni sui trattamenti in corso su di essi;
2) La rettifica o l'aggiornamento dei dati personali trattati, laddove fossero incompleti o non aggiornati;
3) La cancellazione dei dati personali dai database, laddove ritenesse il trattamento non necessario o illegittimo;
4) La limitazione del trattamento dei dati personali, laddove ritenesse che questi non siano corretti, necessari o siano illegittimamente trattati, o laddove si fosse opposto al loro trattamento;
5) La notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;
6) La portabilità dei dati, ossia di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico una copia dei dati personali forniti che lo riguardano, o di richiederne la trasmissione ad un altro Titolare;
7) Di opporsi al trattamento dei dati personali.

Per consentire un più celere riscontro delle richieste formulate nell'esercizio dei suddetti diritti, le stesse potranno essere rivolte inviando anche copia di un documento di identità, all'indirizzo postale della sede legale o all'indirizzo mail: info@uovabelmonte.it.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.4.8 TUTELA DEI MINORI

Al fine di garantire la tutela dei minori, i prodotti e/o servizi resi dalla ditta che possano determinare il porre in essere di potenziali obbligazioni contrattuali, sono riservati a soggetti giuridicamente "abilitati" nella misura in cui sulla base della normativa di riferimento, vengono rispettati i limiti, le modalità e i criteri di identificazione di soggetti "minori" e "non", nonché tutela di questi ultimi. In attuazione dell'art. 8, paragrafo 1, del Regolamento (UE) 2016/679, il minore che abbia compiuto i sedici anni può esprimere il consenso al trattamento dei propri dati personali. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a sedici anni, fondato sull'art. 6, paragrafo 1, lettera a), del Regolamento (UE) 2016/679, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale (Art. 2-quinquies). In ottemperanza a quanto riportato in merito alla tutela dei minori, occorre specificare che il D.Lgs 101/2018 in attuazione di quanto già espresso dal Regolamento UE 2016/679 ha di fatto abbassato il limite anagrafico ad anni quattordici per richiedere per minori di età inferiore il consenso di chi ne esercita la responsabilità genitoriale.

◯**Acconsento** ◯**Non acconsento**

3.5 GESTIONE FORNITORI

Il processo prevede il trattamento dei dati relativi alla gestione dei fornitori con cui la ditta instaura un rapporto di collaborazione, commerciali e lavorativi inerenti il perseguimento del proprio "core business". Principalmente dovranno essere gestiti i fornitori di servizi e/o prodotti con i quali si instaurano rapporti di reciproco interesse commerciale che possano determinare l'acquisizione, gestione, elaborazione e trasmissione di dati. Tale procedura operativa deve avere focus essenziale in primo luogo per tipologia di dati definibili personali ovvero dati che identificano univocamente persone fisiche. Sono da intendersi non strettamente indispensabili i processi per cui vengono acquisiti, gestiti, elaborati e trasmessi dati di natura commerciale, in tal senso la volontà di inserire in operatività di gestione le tipologie di fornitori per cui sussiste il trattamento di dati non personali viene ad identificarsi quale buona prassi aziendale.

3.5.1 FINALITÀ DEL TRATTAMENTO DEI DATI RACCOLTI DAI FORNITORI

I dati personali raccolti possono essere utilizzati per una serie di finalità rivolte al rapporto contrattuale instaurato con il fornitore, ovvero per rispondere a diverse esigenze riscontrabili e di seguito indicate:

1) archiviazione e gestione dei dati inerenti fornitori;
2) conformità degli obblighi e degli adempimenti (amministrativi, fiscali, contabili, etc.) disposti dalla legislazione vigente.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯Acconsento ◯Non acconsento

3.5.2 BASE GIURIDICA DEL TRATTAMENTO

Il trattamento dei dati viene effettuato sulla base giuridica dell'esecuzione di misure contrattuali adottate, ovvero per adempiere ad un obbligo legale con il consenso prestato dall'interessato, in ogni momento liberamente revocabile.

Nel registro dei trattamenti, redatto a cura del titolare del trattamento, vi è riportata apposita sezione nella quale per ogni processo gestito si dovrà indicare ai sensi dell'art.6 (base giuridica su cui si fonda il trattamento) ed al contempo art. 9 (base giuridica per il trattamento di particolari categorie di dati) la base giuridica sulla quale si basa il trattamento dei dati raccolti.

In dettaglio si segua la tabella riportata:

ATTIVITÀ	BASE GIURIDICA (art.6)	BASE GIURIDCA (art.9)
Gestione fornitori	Consenso dell'interessato Esecuzione di un contratto Obbligo legale Legittimo interesse del Titolare	Consenso dell'interessato

3.5.3 PROTEZIONE DEI DATI E TRASFERIMENTO DEI DATI PERSONALI

La protezione dei dati raccolti si realizza, mediante idonee misure di sicurezza, considerando la natura, l'oggetto, il contesto, le finalità del trattamento ed anche il rischio di probabilità e/o gravità di lesione dei diritti e delle libertà delle persone fisiche. Tutti i dati vengono trattati nel massimo rispetto della legge: sottoposti ad aggiornamenti e conservazione in tempi strettamente necessari, secondo tempistica prevista dalla legge. L'acquisizione e la gestione dei dati inerenti i clienti avviene per le finalità descritte, ovvero:

- ✓ archiviazione e gestione dei dati inerenti clienti;
- ✓ conformità degli obblighi e degli adempimenti (amministrativi, fiscali, contabili, etc.) disposti dalla legislazione vigente.

Quanto posto in essere è assimilabile all'acquisizione di dati inerenti principalmente fornitori identificabili in soggetti giuridici (società e affini) e in persone fisiche (secondo necessità ad esempio in caso di consulenti esterni fornitori di servizi dotati di propria partita IVA in forma di ditta individuale). Quanto esplicitato ha obiettivo di identificare i dati acquisiti in informazioni necessarie al conseguimento delle finalità descritte per fini di natura commerciale. I rapporti commerciali tra la ditta e i fornitori si esplicano sia sul territorio nazionale +. In tal modo l'acquisizione e gestione dei dati per finalità di natura commerciale, e qualora necessario dei dati personali, viene effettuata sul territorio nazionale italiano in accordo ed applicazione con quanto disciplinato dal Reg. UE 2016/679 e D.Lgs 101/2018. Pertanto non si procede con il trasferimento di dati verso paesi terzi. Si specifica che in accordo con quanto disciplinato dalla normativa di riferimento il trasferimento di dati personali da paesi appartenenti all´UE verso Paesi "terzi" (non appartenenti all´UE o allo Spazio Economico Europeo) è vietato (articolo 25, comma 1, della Direttiva 95/46/CE), a meno che il Paese in questione non garantisce un livello di protezione "adeguato". In tal senso la Commissione Europea ha stabilito tale adeguatezza attraverso specifiche decisioni (di cui articolo 25, comma 6, della Direttiva 95/46/CE). In deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall´articolo 26, comma 1, della Direttiva 95/46 (consenso della persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, ecc.), nonché sulla base di strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46). La Commissione Europea può stabilire, che il livello di protezione offerto in un determinato Paese risulti adeguato (articolo 25, comma 6, della Direttiva 95/46/CE), e che pertanto è possibile trasferirvi dati personali. Le decisioni definite dalla Commissione Europea definiscono specifici accordi con i paesi di

seguito elencati, mediante le decisioni della Commissione pubblicate in materia di adeguatezza di Paesi terzi. Di seguito i paesi terzi interessati e le relative decisioni e azioni intraprese dalla Commissione Europea, specificando che qualora si renda necessario il trasferimento di dati verso paesi terzi verranno poste in essere le indicazioni operative esplicitate nelle seguenti decisioni della Commissione Europea, di seguito:

- ✓ Andorra (2010/625/UE: Decisione della Commissione, del 19 ottobre 2010, ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali ad Andorra);
- ✓ Argentina (Decisione della Commissione conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina - 30 giugno 2003);
- ✓ Australia (Accordo Europa – Australia, PNR);
- ✓ Canada (2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act);
- ✓ Faer Øer (2010/146/: Decisione della Commissione, del 5 marzo 2010 , ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione fornita dalla legge delle Isole FaerØer sul trattamento dei dati personali);
- ✓ Guernsey (2003/821/CE: Decisione della Commissione, del 21 novembre 2003, sulla adeguata protezione dei dati personali in Guernsey);
- ✓ Isola di Man (Commission decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man);
- ✓ Israele (2011/61/EU: Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data);
- ✓ Jersey (2008/393/CE: Decisione della Commissione, dell' 8 maggio 2008 , ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali a Jersey);
- ✓ Nuova Zelanda (DECISIONE-DELLA-COMMISSIONE-2013-65-UE-Nuova-Zelanda);
- ✓ Svizzera (Decisione della Commissione riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE - 26 luglio 2000);
- ✓ Uruguay (2012/484/EU: Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data);
- ✓ USA: Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull´adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy. (Privacy Shield);
- ✓ USA (USA – PNR: Commissione - Decisione 14 maggio 2004 Customs and Border Protection);
- ✓ Decisione di esecuzione (UE) 2016/2295 della Commissione, del 16 dicembre 2016, che modifica le decisioni 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE e le decisioni di esecuzione 2012/484/UE, 2013/65/UE

riguardanti l´adeguatezza della protezione dei dati personali da parte di taluni paesi, a norma dell´articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio;

Il processo di trattamento dei dati si realizza in completa sicurezza in modo da impedire l'accesso a soggetti terzi.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.5.4 QUALI DATI SONO RACCOLTI

I dati raccolti possono includere riferimenti a:

1) Dati anagrafici (se necessario in riferimento a persone fisiche): Nome, Cognome, Data e Luogo di nascita, Residenza;
2) Ragione sociale (persone giuridiche);
3) Cod. Fiscale e/o Partita IVA (engl. Version: TIN (or EU TIN), VAT Identification Number, and/or equivalent fiscal number for European and non-European country);
4) Recapito telefonico;
5) Recapito e-mail.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯ **Acconsento** ◯**Non acconsento**

3.5.5 TERMINI DI CONSERVAZIONE DEI DATI PERSONALI DELL'UTENTE

La conservazione dei dati si realizza, nel rispetto degli obblighi di legge, per rispondere a richieste di chiarimenti/risoluzioni di eventuali controversie e tutelare i legittimi interessi del titolare del trattamento e dell'interessato. Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la pressi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.5.6 SOGGETTI CON CUI CONDIVIDERE I DATI PERSONALI

I dati acquisiti potranno essere comunicati ai seguenti soggetti:

3) Soggetti terzi che ne hanno necessità secondo obblighi di legge e/o secondo richieste esplicite;
4) Laddove esista l'obbligo di comunicare o condividere i dati personali dell'utente per ottemperare a un obbligo di legge, per darvi applicazione o per indagare, con gli enti di polizia giudiziaria preposti, su violazioni vere o presunte.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯Acconsento ◯Non acconsento

3.5.7 DIRITTI DELL'INTERESSATO

L'interessato ha il diritto di chiedere in qualsiasi momento:

1) L'accesso ai dati personali, (e/o una copia di tali Dati Personali), nonché ulteriori informazioni sui trattamenti in corso su di essi;
2) La rettifica o l'aggiornamento dei dati personali trattati, laddove fossero incompleti o non aggiornati;
3) La cancellazione dei dati personali dai database, laddove ritenesse il trattamento non necessario o illegittimo;
4) La limitazione del trattamento dei dati personali, laddove ritenesse che questi non siano corretti, necessari o siano illegittimamente trattati, o laddove si fosse opposto al loro trattamento;
5) La notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;
6) La portabilità dei dati, ossia di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico una copia dei dati personali forniti che lo riguardano, o di richiederne la trasmissione ad un altro Titolare;
7) Di opporsi al trattamento dei dati personali.

Per consentire un più celere riscontro delle richieste formulate nell'esercizio dei suddetti diritti, le stesse potranno essere rivolte inviando anche copia di un documento di identità, all'indirizzo postale della sede legale o all'indirizzo mail: info@uovabelmonte.it.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯Acconsento ◯Non acconsento

3.6 GESTIONE VIDEOSORVEGLIANZA

La gestione delle attività di videosorveglianza, durante la quale viene effettuata la raccolta dei dati, riguarda le attività svolte presso la sede operativa della ditta.

Pertanto il processo relativo alla gestione della videosorveglianza si esplica mediante il trattamento di dati riconducibili a file video e immagini.

3.6.1 FINALITÀ DEL TRATTAMENTO DEI DATI RACCOLTI

I dati personali raccolti possono essere utilizzati per una serie di finalità relative la gestione delle attività svolte presso la ditta:

1) migliorare la sicurezza all´interno o all´esterno dell'edificio ove si svolgono attività produttive, commerciali;
2) agevolare l´eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

Al termine del processo che richiede la fornitura di dati da parte dell'interessato e pertanto prima dell'acquisizione del dato la prassi operativa aziendale richiede che venga esplicitato il consenso "informato".

◯**Acconsento** ◯**Non acconsento**

3.6.2 BASE GIURIDICA DEL TRATTAMENTO

Il trattamento dei dati viene effettuato sulla base giuridica dell'esecuzione di misure atte ad adempiere ad un obbligo legale con il consenso prestato dall'interessato, in ogni momento liberamente revocabile.

Nel registro dei trattamenti, redatto a cura del titolare del trattamento, vi è riportata apposita sezione nella quale per ogni processo gestito si dovrà indicare ai sensi dell'art. 6 (base giuridica su cui si fonda il trattamento) ed al contempo art. 9 (base giuridica per il trattamento di particolari categorie di dati) la base giuridica sulla quale si basa il trattamento dei dati raccolti.

In dettaglio si segua la tabella riportata:

ATTIVITÀ	BASE GIURIDICA (art.6)	BASE GIURIDCA (art.9)
Gestione videosorveglianza	Consenso dell'interessato Obbligo legale Legittimo interesse del Titolare	Consenso dell'interessato Esercizio obblighi in materia di diritto del lavoro Esercizio obblighi in materia di protezione sociale

3.6.3 PROTEZIONE DEI DATI

La protezione dei dati raccolti si realizza, mediante idonee misure di sicurezza, considerando la natura, l'oggetto, il contesto, le finalità del trattamento ed anche il rischio di probabilità e/o gravità di lesione dei diritti e delle libertà delle persone fisiche.

Tutti i dati personali vengono trattati nel massimo rispetto della legge: sottoposti ad aggiornamenti e conservazione in tempi strettamente necessari all'erogazione dei servizi richiesti dall'interessato, secondo i tempi massimi previsti dalla legge.

Il processo di trattamento si realizza in completa sicurezza in modo da impedire l'accesso a soggetti terzi; al contempo vengono garantiti e mai tralasciati i diritti dell'interessato, di cui:

1) Diritto di accesso (ART. 15)
2) Diritto di rettifica (ART. 16)
3) Diritto di cancellazione (diritto all'oblio) (ART. 17)
4) Diritto di limitazione del trattamento (ART. 18)
5) Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (ART. 19)
6) Diritto alla portabilità dei dati (ART. 20)
7) Diritto di opposizione (ART. 21)

3.6.4 QUALI DATI PERSONALI SONO RACCOLTI

I dati personali raccolti possono includere riferimenti a file video e immagini, che al contempo permettono l'identificazione di persone fisiche. La raccolta dei dati avviene successivamente al consenso informato mediante l'apposizione di informativa nei luoghi protetti da videosorveglianza e comunque prima che la persona fisica rientri nel campo d'azione degli apparati di ripresa video.

3.6.5 TERMINI DI CONSERVAZIONE DEI DATI PERSONALI DELL'UTENTE

La conservazione dei dati personali si realizza nelle modalità e tempistiche previste nel rispetto degli obblighi di legge, nonché al contempo per la risoluzione di eventuali controversie e tutelare i legittimi interessi del titolare del trattamento e dell'interessato. Le immagini risultano presenti in formato digitale per 24 ore successivamente vengono sovrascritte.

3.6.6 SOGGETTI CON CUI CONDIVIDERE I DATI PERSONALI

I dati personali dell'interessato possono essere condivisi con i seguenti soggetti:

1) Soggetti terzi che ne hanno necessità secondo obblighi di legge e/o secondo richieste esplicite (a titolo esemplificativo si considerano INPS, INAIL, Direzione Provinciale del Lavoro, Organi di Vigilanza);
2) Laddove esista l'obbligo di comunicare o condividere i dati personali dell'utente per ottemperare a un obbligo di legge, per darvi applicazione o per indagare, con gli enti di polizia giudiziaria preposti, su violazioni vere o presunte.

3.6.7 DIRITTI DELL'INTERESSATO

L'interessato ha il diritto di chiedere in qualsiasi momento:

1) L'accesso ai dati personali, (e/o una copia di tali Dati Personali), nonché ulteriori informazioni sui trattamenti in corso su di essi;
2) La rettifica o l'aggiornamento dei dati personali trattati, laddove fossero incompleti o non aggiornati;
3) La cancellazione dei dati personali dai database, laddove ritenesse il trattamento non necessario o illegittimo;
4) La limitazione del trattamento dei dati personali, laddove ritenesse che questi non siano corretti, necessari o siano illegittimamente trattati, o laddove si fosse opposto al loro trattamento;
5) La notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;
6) La portabilità dei dati, ossia di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico una copia dei dati personali forniti che lo riguardano, o di richiederne la trasmissione ad un altro Titolare;
7) Di opporsi al trattamento dei dati personali.

Per consentire un più celere riscontro delle richieste formulate nell'esercizio dei suddetti diritti, le stesse potranno essere rivolte inviando anche copia di un documento di identità, all'indirizzo postale della sede legale o all'indirizzo mail: info@uovabelmonte.it.

3.6.8 TUTELA DEI MINORI

In attuazione dell'art. 8, paragrafo 1, del Regolamento (UE) 2016/679, il minore che ha compiuto i sedici anni può esprimere il consenso al trattamento dei propri dati personali. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a sedici anni, fondato sull'art. 6, paragrafo 1, lettera a), del Regolamento (UE) 2016/679, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale. (Art. 2-quinquies - Consenso del minore in relazione ai servizi della società dell'informazione).

In ottemperanza a quanto riportato in merito alla tutela dei minori, occorre specificare che il D.Lgs 101/2018 in attuazione di quanto già espresso dal Regolamento UE 2016/679 ha di fatto abbassato il limite anagrafico ad anni quattordici per richiedere per minori di età inferiore il consenso di chi ne esercita la responsabilità genitoriale.

4 GUIDA ALL'UTILIZZO DEL MANUALE DELLA PRIVACY

PREMESSA

L'introduzione della normativa europea sulla privacy (General Data Protection Regulation – GDPR) impone regole nuove, per cui risulta necessario definire ruoli, procedure e documentazioni per la loro corretta applicazione.

Per facilitare la realizzazione di tale attività, si propongono le informazioni necessarie e gli strumenti utili in funzione di una rigorosa attenzione dei dati trattati e dei processi.

Gli step operativi di gestione verranno organizzate nelle seguenti fasi:

1) **ANAGRAFICA**: in questa sezione dovranno essere inseriti i dati anagrafici della ditta;
2) **PERSONALE**: in questa sezione dovranno essere indicati i nominativi dei dipendenti;
3) **FORNITORI**: in questa sezione dovranno essere elencati i nominativi dei fornitori che trattano dati personali, altra tipologia di fornitori è ammessa ma non strettamente necessaria;
4) **CLIENTI**: in questa sezione dovranno essere elencati i nominativi dei soli clienti per i quali si pone in essere il processo di trattamento di dati;
5) **PROCESSI**: questa sezione deve includere tutti i processi potenzialmente attivi, per ognuno dei quali vengono individuate le caratteristiche standard rispetto al trattamento dei dati;
6) **ACCONTABILITY**: in questa sezione il titolare del trattamento dei dati potrà associare ad ogni processo i rispettivi incaricati del trattamento.

Al termine di queste operazioni sarà possibile gestire il relativo Registro dei trattamenti.

ANAGRAFICA

La sezione "Anagrafica" costituisce una delle prime sezioni che deve essere compilata, ed in essa è possibile effettuare la seguente distinzione:

1) **Informazioni generali**: informazioni riguardanti l'azienda in oggetto di analisi;
2) **Informazioni del Titolare del trattamento dei dati**;
3) **Informazioni del Responsabile del trattamento dei dati**;
4) **Informazioni del Responsabile della protezione dai dati**.

Informazioni generali

Denominazione	Società Agricola Semplice Belmonte di Mazzilli Rosa Anna
Indirizzo (sede legale e sede operativa)	Via Pitagora, 30 – Corato (BA) S.P. 231 Parco del fornello – Ruvo di Puglia (BA)
Città	Ruvo di Puglia
Provincia	BA
Cap	70037
Tipologia	Società in accomandita semplice
Codice Fiscale	06717410721
Partita Iva	06717410721

Informazioni del Titolare del trattamento dei dati

Denominazione	Società Agricola Semplice Belmonte di Mazzilli Rosa Anna
Indirizzo (sede legale e sede operativa)	Via Pitagora, 30 – Corato (BA) S.P. 231 Parco del fornello – Ruvo di Puglia (BA)
Città	Ruvo di Puglia
Provincia	BA
Cap	70037
Tipologia	Società in accomandita semplice
Codice Fiscale	06717410721
Partita Iva	06717410721

Informazioni del Responsabile del trattamento dei dati

Denominazione	Sig.ra Mazzilli Rosa Anna
Indirizzo (sede legale e sede operativa)	Via Pitagora, 30 – Corato (BA) S.P. 231 Parco del fornello – Ruvo di Puglia (BA)
Città	Ruvo di Puglia
Provincia	BA
Cap	70037
Tipologia	Persona fisica
Codice Fiscale	MZZRNN66R56C514I
Partita Iva	---

Informazioni del Responsabile della protezione dei dati

Denominazione	Non necessario e non nominato
Indirizzo (sede legale)	---
Città	---
Provincia	---
Cap	---
Indirizzo (sede operativa inerente lo svolgimento dell'incarico)	---
Città	---
Provincia	---
Cap	---

PERSONALE

Nella seguente sezione viene chiarita la modalità di inserimento dei dati anagrafici e delle corrispettive mansioni dei dipendenti.

L'inserimento dei dati dei dipendenti permette la gestione del dato personale (dell'interessato) in sé ed al contempo permette l'identificazione del personale che interviene nei processi di acquisizione, gestione ed archiviazione dei dati, pertanto nel/i processo/i di trattamento del/i dato/i.

La compilazione del seguente format risulta indispensabile per la successiva fase di "Accountability" (designazione del responsabile per ogni singolo processo), l'inserimento dei dati relativi viene effettuato in occasione della redazione del registro dei trattamenti.

Nome	Cognome	Data di nascita	Luogo di nascita	Codice Fiscale	Mansione

FORNITORI

La conoscenza dettagliata dei fornitori, attraverso la raccolta delle rispettive informazioni, consente di analizzare ogni tipologia di dato trattato senza considerare quelli riferibili ai servizi che non trattano dati sensibili. Anche per la gestione dei dati inerenti i fornitori si prevede la fornitura dell'informativa in merito alle policy aziendali di gestione della privacy, l'inserimento dei dati relativi viene effettuato in occasione della redazione del registro dei trattamenti.

Identificativo fornitore	Tipologia di Servizi	Consegna informativa	
		Si	No

CLIENTI

La conoscenza dettagliata dei clienti, attraverso la raccolta delle rispettive informazioni, consente di analizzare ogni tipologia di dato trattato nelle modalità e tempistiche propedeutiche all'erogazione di un servizio, vendita di prodotti e per i fini contabili ed amministrativi consentiti dalla normativa di riferimento. Anche per la gestione dei dati inerenti i clienti si prevede la fornitura dell'informativa in merito alle policy aziendali di gestione della privacy, l'inserimento dei dati relativi viene effettuato in occasione della redazione del registro dei trattamenti.

Identificativo cliente	Consegna informativa	
	Si	No

PROCESSI

Nella seguente sezione verranno inseriti tutti i processi aziendali i cui "argomenti" specifici richiedono l'acquisizione e gestione del dato. Un vero e proprio elenco dei processi aziendali correlati ai relativi dati trattati, che consente la successiva gestione del Registro dei trattamenti.

Processo Aziendale	Oggetto del Trattamento dati
Gestione sito web	attività di richiesta di informazioni, assistenza clienti
Gestione social network	gestione richiesta di informazioni
Gestione risorse umane	gestione processi inerenti le risorse umane ed organizzazione dei dipendenti
Gestione clienti	gestione attività contabili ed amministrative
Gestione fornitori	gestione attività contabili ed amministrative
Gestione videosorveglianza	gestione attività di acquisizione dati video e immagini per sicurezza dei lavoratori e sicurezza patrimonio aziendale

ACCOUNTABILITY

L'esigenza, soddisfatta dall'introduzione del principio di responsabilizzazione, è quella di far in modo che i soggetti che determinano le finalità ed i mezzi del trattamento, o che trattano i dati per loro conto, dunque il titolare ed il responsabile del trattamento, definiscano tutte le misure necessarie alla protezione effettiva del dato personale oggetto dei trattamenti. Quanto richiesto ai titolari ed ai responsabili del trattamento è un approccio proattivo con focus su obblighi e comportamenti che prevengano in modo effettivo il possibile evento di danno, configurandosi sulle specificità dei diversi trattamenti cui si riferiscono. Il dato inserito nella gestione di un processo aziendale che richiede il trattamento del dato sarà desunto e risulterà corrispondente a quanto indicato in tabella relativa al "PERSONALE" precedentemente compilata.

Pertanto si prevede la compilazione del seguente format che diviene parte integrante del registro dei trattamenti, l'inserimento dei dati relativi viene effettuato in occasione della redazione del registro dei trattamenti.

Processo	Nome	Cognome	Mansione
Gestione sito web	Si veda Registro dei Trattamenti		
Gestione social network			
Gestione risorse umane			
Gestione clienti			
Gestione fornitori			
Gestione videosorveglianza			

QUESTIONARIO

Successivamente alla compilazione della Sezione "Accountability", è possibile procedere con la compilazione di un questionario il cui fine è quello di porre in essere i requisiti essenziali per la compilazione del Registro dei Trattamenti.

Le domande trattate vengono poste con relative risposte chiuse (SI, NO, NON SO) e riguardano i processi indicati al paragrafo precedente.

Quesito	Risposta
I dati trattati sono conservati in sicurezza?	X**SI**◯**NO**◯**NON SO**
I sistemi ICT dispongono di firewall?	X**SI**◯**NO**◯**NON SO**
I vari sistemi (elettronico, informatico e connettività) sono adeguatamente ridondati?	X**SI**◯**NO**◯**NON SO**
Le password sono periodicamente modificate?	X**SI** ◯**NO**◯**NON SO**
Le password sono conservate in modo riservato e sicuro?	X**SI**◯**NO**◯**NON SO**
I ruoli del personale rispetto alla privacy sono stati definiti in modo chiaro?	X**SI**◯**NO**◯**NON SO**
Il personale è stato formato in modo specifico?	X**SI**◯**NO**◯**NON SO**
Il personale segue un codice di condotta?	X**SI**◯**NO**◯**NON SO**
I dati sono trattati solo per lo specifico fine del processo?	X**SI**◯**NO**◯**NON SO**
E' garantito il diritto di accesso?	X**SI**◯**NO**◯**NON SO**
E' garantito il diritto di rettifica?	X**SI**◯**NO**◯**NON SO**

DATA BREACH

Per "**Data Breach"** si intende una violazione accidentale o fraudolenta della sicurezza dei dati a seguito di una distruzione, alterazione, accesso o divulgazione non autorizzati a dati personali trasmessi, archiviati, divulgati o altrimenti processati.

Si identificano 3 tipologie generali di Data Breach:

1. **VIOLAZIONE DI CONFIDENZIALITÀ**: accesso e/o divulgazione non autorizzata di dati personali;
2. **VIOLAZIONE DI INTEGRALITÀ**: alterazione non autorizzata o accidentale di dati personali;
3. **VIOLAZIONE DI DISPONIBILITÀ**: perdita di accesso e/o distruzione di dati personali non autorizzata o accidentale.

Il Titolare del trattamento dei dati è tenuto ad informare l'Autorità di controllo e l'interessato (a cui i dati fanno riferimento) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

In caso di rilevata violazione secondo le tipologie descritte è necessario compilare il seguente questionario, indicando la tipologia di violazione rilevata, ed indicare il livello di gravità.

Lettura non autorizzata	◯**M.A.**◯**A**◯**M**◯**B/T**
Copia (i dati copiati non sono stati alterati e sono ancora presenti in memoria/archivio)	◯**M.A**. ◯**A**◯**M**◯**B/T**
Furto (copia e cancellazione – i dati copiati non sono più presenti in memoria/archivio)	◯**M.A.**◯**A**◯**M**◯**B/T**
Alterazione (i dati sono stati alterati ma non copiati)	◯**M.A.**◯**A**◯**M**◯**B/T**
Perdita (i dati sono stati cancellati dalla memoria o non sono più presenti in archivio, ma non sono stati copiati)	◯**M.A.**◯**A**◯**M**◯ **B/T**
Distruzione (malfunzionamento) totale o parziale dei supporti informatici/archivio	◯**M.A.**◯**A**◯**M**◯**B/T**
Smarrimento/furto di supporti informatici (hard disk, chiavette USB, ecc…)	◯**M.A.**◯**A**◯**M**◯**B/T**

LEGENDA:

- **M.A**. = Molto Alto
- **A** = Alto
- **M** = Medio
- **B/T** = Basso/Trascurabile