



REGOLAMENTO AZIENDALE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sulla base del Regolamento Europeo 679/2016 (GDPR)
e dalle successive integrazioni e indicazioni del Garante per la Privacy

SOMMARIO

PARTE PRIMA: INTRODUZIONE.....	4
ARTICOLO 1. PREMESSA DI CARATTERE NORMATIVO.....	4
ARTICOLO 2. PREMESSA DI CARATTERE ORGANIZZATIVO.....	4
ARTICOLO 3. PREMESSA DI CARATTERE METODOLOGICO.....	4
PARTE SECONDA: DISPOSIZIONI GENERALI	5
ARTICOLO 4. OGGETTO DEL REGOLAMENTO	5
ARTICOLO 5. FINALITÀ' DEL REGOLAMENTO.....	5
ARTICOLO 6. SENSIBILIZZAZIONE	5
ARTICOLO 7. DEFINIZIONI	6
ARTICOLO 8. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI	7
ARTICOLO 9. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI	8
ARTICOLO 10. TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI).....	8
ARTICOLO 11. COMUNICAZIONE DI DATI VERSO L'ESTERNO	8
ARTICOLO 12. DOSSIER SANITARIO ELETTRONICO AZIENDALE	8
ARTICOLO 13. TRATTAMENTO DEI DATI DEI DIPENDENTI	10
Articolo 14. Trattamento dati affidati all'esterno.....	10
PARTE TERZA: DIRITTI DELL'INTERESSATO.....	11
ARTICOLO 15. INFORMATIVA SUL TRATTAMENTO DEI DATI.....	11
ARTICOLO 16. CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI	12
ARTICOLO 17. DIRITTO DI ACCESSO DELL'INTERESSATO	12
ARTICOLO 18. DIRITTO DI RETTIFICA	14
ARTICOLO 19. DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)	14
ARTICOLO 20. DIRITTO DI LIMITAZIONE AL TRATTAMENTO.....	14
ARTICOLO 21. DIRITTO ALLA PORTABILITA' DEI DATI	14
ARTICOLO 22. DIRITTO DI OPPOSIZIONE	15
ARTICOLO 23. PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)	15
PARTE QUARTA TITOLARE E RESPONSABILE DEL TRATTAMENTO.....	15
ARTICOLO 24. TITOLARE DEL TRATTAMENTO.....	15
ARTICOLO 25. CONTITOLARI DEL TRATTAMENTO	16
ARTICOLO 26. RESPONSABILE INTERNO DEL TRATTAMENTO DEI DATI	16
ARTICOLO 27. RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI	17
ARTICOLO 28. INCARICATO (AUTORIZZATO) INTERNO ED ESTERNO DEL TRATTAMENTO DEI DATI.....	19
ARTICOLO 29. RESPONSABILE AZIENDALE DELLA PROTEZIONE DEI DATI.....	19
PARTE QUINTA: SICUREZZA DEI DATI PERSONALI MISURE DI CARATTERE INFORMATICO E TECNOLOGICO.....	20
ARTICOLO 30. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA	20
ARTICOLO 31. REGISTRO ELETTRONICO DELLE ATTIVITA' DI TRATTAMENTO	21
ARTICOLO 32. PROTEZIONE E SICUREZZA DEI DATI PERSONALI	21
ARTICOLO 33. NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO	21
ARTICOLO 34. VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI.....	22

ARTICOLO 35. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO	22
ARTICOLO 36. DISCIPLINA AZIENDALE SULLA VIDEOSORVEGLIANZA	22
ARTICOLO 37. DISCIPLINA AZIENDALE SULL'UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI	22
PARTE SESTA	23
ATTUAZIONE IN AMBITO AZIENDALE DEGLI ADEMPIMENTI EUROPEI	23
ARTICOLO 38. AMBITI DI ATTIVITÀ AZIENDALI CORRELATI AI NUOVI OBBLIGHI EUROPEI	23
ARTICOLO 39. ENTRATA IN VIGORE E PUBBLICITÀ	23
ARTICOLO 40. DISPOSIZIONE FINALE RELATIVA AGLI "ALLEGATI TECNICI"	24

ALLEGATI AL REGOLAMENTO AZIENDALE

- 1) Deliberazione del CdA del 26/03/2018, ad oggetto: *"Prime azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'Associazione Primavera Onlus, agli obblighi del Regolamento Europeo n. 2016/679 sulla privacy"*; Deliberazione del CdA del 21/05/2018, ad oggetto: *"adozione del Regolamento interno sulla Privacy Rev. 0.0 del 11/05/2018"* Deliberazione del CdA del 28/09/2018, ad oggetto: *"aggiornamento del Regolamento interno sulla Privacy Rev. 01 del 20/09/2018"*
- 2) Modulistica aziendale relativa al Dossier Sanitario Elettronico
- 3) Modulistica aziendale relativa all'Informativa e al Consenso al trattamento dei dati
- 4) Format aziendale per la nomina dei Responsabili (Designati) del trattamento dei dati
- 5) Format aziendale per la nomina degli Autorizzati o Incaricati del trattamento dei dati
- 6) Format aziendale per la nomina dei Responsabili Esterni del trattamento dei dati
- 7) Format aziendale per la nomina del Responsabile della Protezione dei Dati
- 8) Modello del Garante per la privacy di notifica del *Data Breach*
- 9) Regolamento aziendale sulla videosorveglianza
- 10) Regolamento aziendale sull'utilizzo dei mezzi informatici e telematici
- 11) Piano di continuità operativa e di disaster recovery
- 12) Procedure operative come elencate di seguito:
 - GDPR PO Pri - 2.0 rev0 - obblighi generali
 - GDPR PO Pri - 2.1 rev0 - Gestione sistemi informatici
 - GDPR PO Pri - 2.2 rev0 - Gestione delle misure di sicurezza
 - GDPR PO Pri - 2.3 rev0 - Accesso alle risorse informatiche e di rete
 - GDPR PO Pri - 2.4 rev0 - Classificazione dei documenti
 - GDPR PO Pri - 2.5 rev0 - Gestione back up
 - GDPR PO Pri - 2.6 rev0 - Gestione degli incidenti
 - GDPR PO Pri - 2.7 rev0 - Gestione della navigazione
 - GDPR PO Pri - 2.8 rev0 - Gestione della posta
 - GDPR PO Pri - 2.9 rev0 - Gestione della rete
 - GDPR PO Pri - 3.0 rev0 - Gestione delle utenze
 - GDPR PO Pri - 3.1 rev0 - sviluppo software
 - GDPR PO Pri - 3.2 rev0 - Violazione dei dati personali
 - GDPR PO Pri - 3.3 rev0 - Classificazione dei dati

PARTE PRIMA: INTRODUZIONE

ARTICOLO 1. PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento in materia di protezione dei dati personali (così detta “privacy”) è uno strumento di applicazione del vigente Decreto Legislativo 30 giugno 2003, n. 196 così come novellato dal D.Lgs 10 agosto 2018 N. 101 e, in particolare, del nuovo Regolamento Europeo n. 2016/679, nell'ambito dell'organizzazione dell'Associazione Primavera Onlus.

A far data dal 25 maggio 2018 trova diretta applicazione, sul territorio nazionale, l'anzidetto, nuovo Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

La sua entrata in vigore è stabilita il 24 maggio 2016: entro due anni a partire da tale data, e quindi entro la data del 25 maggio 2018, tutti gli Stati membri dell'Unione debbono uniformarsi alle nuove regole comunitarie, evitando così di incorrere nelle pesanti sanzioni (sia economiche sia di natura penale) previste dalla nuova normativa.

E' necessario pertanto, come Azienda, dotarsi di un apposito “Regolamento” che disciplini compiti, attività e *policy* interne che garantiscano l'assolvimento dei (non pochi) adempimenti imposti dalle norme europee.

Il presente Regolamento aziendale si rende inoltre necessario per recepire, in un unico testo, i precetti normativi a maggior rilevanza, sia di carattere aziendale che nazionale in tema di trattamento dei dati personali (*D.lgs. 196 del 30/06/2003 come modificato dal D.Lgs 10 agosto 2018 N. 101, regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttiva dell'UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche e soprattutto Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*).

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

ARTICOLO 2. PREMESSA DI CARATTERE ORGANIZZATIVO

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per l'utente/assistito che si rivolge alla struttura aziendale, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell'essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità del singolo individuo.

Per questi motivi, la “cultura della privacy” necessita di divenire un vero e proprio elemento cardine dell'organizzazione di questa azienda, che deve impegnarsi perché la cultura di cui si tratta possa crescere e rafforzarsi, in quanto solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di carattere tecnico ed organizzativo, nel trattamento dei dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza e gli assistiti.

ARTICOLO 3. PREMESSA DI CARATTERE METODOLOGICO

Vengono allegati a questo Regolamento una serie di **documenti tecnici** necessari a dare compiuta attuazione, sia verso l'interno che verso l'esterno, ai dettami della nuova “privacy europea”: documenti ai

quali viene data massima pubblicità e diffusione, tramite la diffusione nelle sedi aziendali e sul sito *internet* istituzionale.

Tra questi documenti vi sono, a titolo esemplificativo, il modello aziendale di nomina del Responsabile esterno del trattamento dei dati personali, il modulo per l'informativa ed il consenso al trattamento dei dati, la modulistica relativa al Dossier sanitario elettronico ed il disciplinare aziendale sull'utilizzo dei mezzi informatici e telematici dell'azienda.

E' doveroso rimarcare, sin da ora, che il principio cardine introdotto dal nuovo Regolamento UE è quello della **"responsabilizzazione"** (**accountability** nell'accezione inglese) che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della **"conformità"** o **compliance** nell'accezione inglese); vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

Si tratta di una grande novità per la protezione dei dati in quanto 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.

Questa Azienda, nella persona del Suo Legale rappresentante, ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* ed alla *compliance*.

PARTE SECONDA: DISPOSIZIONI GENERALI

ARTICOLO 4. OGGETTO DEL REGOLAMENTO

Il presente Regolamento disciplina, all'interno dell'Associazione Primavera Onlus, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Decreto Legislativo del 30/06/2003 n. 196 così come novellato dal D.Lgs 10 agosto 2018 N. 101 ed in conformità al Regolamento UE n. 679/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

ARTICOLO 5. FINALITÀ' DEL REGOLAMENTO

L'Azienda garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della *Carta dei diritti fondamentali* dell'Unione Europea.)

ARTICOLO 6. SENSIBILIZZAZIONE

L'Associazione Primavera Onlus sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale aziendale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Azienda.

Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza dal presente nuovo Regolamento aziendale, al momento dell'ingresso in servizio è fornita, a cura dell'Ufficio Privacy e Qualità, ad ogni dipendente (*oltre che ad ogni collaboratore o consulente libero*

professionale) una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i soggetti non dipendenti poc'anzi citati), con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali “**incaricati ed autorizzati al trattamento dei dati**” ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679.

Detta comunicazione conterrà anche i riferimenti per reperire il presente Regolamento sul sito internet nonché sullo spazio *intranet* aziendale.

Il Regolamento, pubblicato sul sito aziendale, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

ARTICOLO 7. DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare aziendale si intende per:

- a) «**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;
- b) «**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;
- c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- d) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una 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;
- e) «**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;
- f) «**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;
- g) «**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;
- h) «**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;
- i) «**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;

l) **«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;

m) **«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;

n) **«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;

o) **«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;

p) **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

ARTICOLO 8. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**«liceità, correttezza e trasparenza»**);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali (**«limitazione della finalità»**);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**«minimizzazione dei dati»**).
- d) A tale proposito, il Regolamento UE ricalca i principi sostanziali di **«necessità, pertinenza, indispensabilità e non eccedenza»** (rispetto alle finalità del trattamento) contenuti negli articoli 4 e 11 del D.lgs. 196/2003.
- e) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**«esattezza»**);
- f) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (**«limitazione della conservazione»**);
- g) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**«integrità e riservatezza»**).
- h) Come stabilito dal Regolamento UE, il Titolare del trattamento (Legale Rappresentante dell'Associazione Primavera Onlus) è competente per il rispetto di quanto sin qui esposto ed è in grado di provarlo verso l'esterno (principio europeo dell'**«accountability»** o **«responsabilizzazione»**).

ARTICOLO 9. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'*origine razziale o etnica*, le *opinioni politiche*, le *convinzioni religiose o filosofiche*, o l'*appartenenza sindacale*, nonché trattare *dati genetici*, *dati biometrici* intesi a identificare in modo univoco una persona fisica, *dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, tra le quali si evidenzia quella di cui alla lettera "h", applicabile a questa Azienda, ai sensi della quale *"il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (..)"*.

Si fa presente, inoltre, che il Regolamento UE consente di *"mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute"* (articolo n. 9, paragrafo n. 4).

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati particolari, biometrici e genetici e in particolare con le *"Autorizzazioni generali"*, dall'Autorità Garante per la protezione di dati personali.

ARTICOLO 10. TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, *"il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."*

Si dà atto che l'art. 22 comma 2 del D.lgs 10 agosto 2018 N. 101 modifica l'art. 4 del D.lgs. 196/2003 e che le espressioni «dati sensibili» e «dati giudiziari» di cui al comma 1, lettere d) ed e) ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati giudiziari e in particolare con le *"Autorizzazioni generali"*, dall'Autorità Garante per la protezione di dati personali.

ARTICOLO 11. COMUNICAZIONE DI DATI VERSO L'ESTERNO

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al Capo V del Reg. UE 679/2016.

ARTICOLO 12. DOSSIER SANITARIO ELETTRONICO AZIENDALE

Il Dossier Sanitario Elettronico (abbreviato "D.S.E.") raccoglie l'insieme dei dati personali generati da eventi clinici presenti e trascorsi che riguardano il paziente, messi in condivisione logica al fine di documentarne la storia clinica e di offrirle un migliore processo di cura/assistenza.

Il Dossier Sanitario Elettronico rappresenta un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della terapia prestata all'assistito, volto a documentare parte della storia clinica dell'utente attraverso la realizzazione di un sistema integrato di informazioni circa il relativo stato di salute accessibile dal personale autorizzato.

Ciascuna delle Strutture di questa azienda che si occupa terapia domiciliare con tenuta della cartella clinica già dispone singolarmente della tecnologia digitale indispensabile alla gestione ed archiviazione dei dati sanitari del paziente: relazioni sulle terapie ed ogni altra tipologia di informazione sanitaria; ogni operatore autorizzato può consultare le informazioni sanitarie prodotte dall'equipe ma può modificare soltanto di dati per cui è stato autorizzato ed ha accesso esclusivo con proprie credenziali).

Nel Dossier Sanitario Elettronico, una volta costituito, confluiscono invece tutte le informazioni sanitarie che riguardano uno stesso paziente presenti in questa Azienda. In caso di rifiuto dell'interessato alla costituzione del Dossier Sanitario Elettronico, in nessun modo possono essere prestati i servizi di assistenza domiciliare integrata.

Per poter costituire un Dossier Sanitario Elettronico ed accedere a tutte le informazioni di cui si è detto, secondo normativa vigente e secondo prassi consolidata nell'ambito di questa azienda, è necessario che il paziente rilasci, in forma scritta e dopo aver letto l'apposita nota informativa, il proprio consenso. Resta ferma la possibilità per l'interessato di manifestare di volta in volta, in occasione di ogni singolo evento clinico, il proprio diniego all'inserimento dello stesso nel DSE "oscuramento" dell'evento clinico. Tale volontà è espressa mediante compilazione di specifico modulo fornito dal responsabile della struttura sanitaria complessa che ha fornito la prestazione medica.

L'assistito può, inoltre, decidere, attraverso rilascio di specifico consenso scritto, se inserire o non inserire nel Dossier Sanitario Elettronico le informazioni relative ad eventi sanitari pregressi all'istituzione del Dossier prodotti nell'Associazione Primavera Onlus.

L'Associazione Primavera Onlus assicura, a tutela della riservatezza dell'assistito, che una volta manifestata la volontà del medesimo in merito al trattamento dei dati personali mediante costituzione di Dossier Sanitario Elettronico, lo stesso interessato possa decidere di **oscurare** taluni dati o documenti sanitari consultabili tramite tale strumento.

L' "**Oscureamento**" dell'evento clinico (revocabile nel tempo) avverrà con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire a conoscenza del fatto che l'interessato ha effettuato tale scelta (cd. "*Oscureamento dell'oscuramento*").

Il Dossier è consultabile esclusivamente dal personale sanitario autorizzato della struttura presso la quale il paziente ha rilasciato l'autorizzazione o da altro personale sanitario quando si renda

necessaria una specifica consulenza specialistica concordata con l'interessato.

Il Dossier è consultabile anche da parte dei professionisti che agiscono in regime di *libera professione* ovvero nella erogazione di prestazioni *al di fuori del normale orario di lavoro*

utilizzando anche le proprie strutture.

Criteri di profilazione degli utenti

Per la protezione dei dati personali del paziente da specifici rischi di accesso non autorizzato e di trattamenti non consentiti, il personale sanitario "*Incaricato del Trattamento*" è in possesso di una propria *password* che consente la tracciabilità degli accessi e delle modifiche effettuate, garantendo così anche l'esattezza e l'integrità dei dati.

I server presso cui sono custoditi i dati sono gestiti dalla software house fornitrice del programma applicativo e sono, come dichiarato e sottoscritto, dotati di sistemi di *Back-up* e di sistemi antivirus e anti intrusione.

I dati personali utilizzati per la costituzione del Dossier Sanitario Elettronico vengono trattati rispettando i principi di correttezza, liceità, necessità e finalità stabiliti dal Decreto Legislativo 196/2003 così come novellato dal D.Lgs 10 agosto 2018, n. 101e osservando le misure di sicurezza previste dall'Allegato "B" - *Disciplinare Tecnico* del medesimo Decreto Legislativo.

Il paziente, in sede di nota informativa, è anche informato del fatto che in qualsiasi momento, rivolgendosi al *Titolare del Trattamento dei dati*, è in grado di (così come previsto dall'articolo 7 del Decreto Legislativo 196/2003):

- **revocare il consenso** ad alimentare il Dossier con l'inserimento di esami o referti ("*istanza di revoca*");

- esercitare la **facoltà di oscurare** eventi clinici che lo riguardano (*"istanza di oscuramento"*);
- **esercitare il diritto di accesso ai dati personali** contenuti nel Dossier Sanitario Elettronico (*"istanza di esercizio dei diritti"*);
- **visionare gli accessi** che sono stati effettuati sul proprio Dossier Sanitario Elettronico da parte dei soggetti abilitati alla consultazione (*"istanza di accesso"*);

ARTICOLO 13. TRATTAMENTO DEI DATI DEI DIPENDENTI

Il trattamento dei dati personali dei dipendenti, aspiranti tali, collaboratori esterni e soggetti equiparati ai dipendenti, avviene esclusivamente per lo svolgimento di finalità istituzionali attinenti all'instaurazione ed intrattenimento dei rapporti di lavoro.

L'Associazione Individua il personale Incaricato a trattare tali dati e assicurare idonee misure di sicurezza per proteggerli da indebite intrusioni o illecite divulgazioni.

Al Dipendente è fornita idonea Informativa sull'uso che verrà fatto dei suoi dati e gli è consentito di esercitare agevolmente i diritti che la normativa sulla privacy gli riconosce (accesso ai dati, aggiornamento, rettifica, cancellazione etc.).

Entro 1 mese dalla richiesta l'Associazione è tenuta a comunicare in modo chiaro tutte le informazioni in suo possesso.

Senza il consenso del dipendente non si possono comunicare informazioni ad associazioni di datori di lavoro, di ex dipendenti o a conoscenti, familiari, parenti.

Il consenso è necessario anche per pubblicare informazioni personali (foto, curricula) nella Intranet aziendale e in Internet.

Nella bacheca aziendale possono essere affissi solo ordini di servizio, turni lavorativi o feriali.

Non si possono invece diffondere emolumenti percepiti, sanzioni disciplinari, assenze per malattia, adesione ad associazioni.

I dati sanitari dei dipendenti sono conservati in fascicoli separati tenuti presso lo studio del Medico Competente.

Il dipendente assente per malattia è tenuto a consegnare al proprio ufficio un certificato senza la diagnosi ma con la sola indicazione dell'inizio e della durata presunta dell'infermità.

L'Associazione non può accedere alle cartelle sanitarie dei dipendenti sottoposti ad accertamenti dal medico del lavoro. Nel caso di denuncia di infortuni o malattie professionali all'INAIL, l'Associazione deve limitarsi a comunicare solo le informazioni connesse alla patologia denunciata.

ARTICOLO 14. TRATTAMENTO DATI AFFIDATI ALL'ESTERNO

In questa sezione è esposto un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Per gli adempimenti di legge, per la gestione dei dati degli interessati o per altre attività dell'Associazione . (es. tenuta del libro unico del lavoro e della documentazione relativa, tenuta delle scritture contabili (contabilità IVA e libri sociali), presa in carico e gestione degli assistiti, etc.), infatti, alcuni dati personali vengono affidati all'esterno e/o co-gestiti con Responsabili esterni del trattamento.

Ai Responsabili esterni nominati, a cui si affida l'incarico, si richiede conformità di trattamento al Regolamento UE 679/2016 e alle norme minime prescritte dal D. Lgs. 196/2003 così come modificato dal D.Lgs n.101 del 10/08/2018 e dall'Allegato B dello stesso.

Gli stessi, infatti, si sono impegnati, in qualità di Responsabile esterno al trattamento dei dati degli Interessati a:

1. adempiere agli obblighi previsti dalla normativa europea e nazionale sulla protezione dei dati personali, poiché i dati che tratterà nell'espletamento dell'incarico ricevuto sono comunque dati personali;
2. trattare i dati al solo fine dell'espletamento dell'incarico ricevuto;
3. rispettare le istruzioni specifiche contenute nella lettera di nomina, conformando ad esse le procedure già eventualmente in essere;
4. relazionare annualmente sulle misure adottate e di avvertire immediatamente i referenti dell'Associazione in caso di situazioni anomale o di emergenza;
5. riconoscere eventualmente il diritto dell'Associazione a verificare periodicamente l'applicazione delle norme di sicurezza adottate;
6. attestare l'adozione delle misure minime di sicurezza previste dall'art. 34 D.lgs. 196/2003 così come modificato da D.Lgs n. 101 del 10/08/2018 e del disciplinare tecnico Allegato B e del Regolamento UE 679/2016.

PARTE TERZA: DIRITTI DELL'INTERESSATO

ARTICOLO 15. INFORMATIVA SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, 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 (R.P.D.);
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- 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 paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni 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 determinare tale periodo;
- 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'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, 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'eventuale esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questa azienda, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore

a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati così come indicato nel **Registro dei Trattamenti**.

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 ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

Alla luce dei principi esposti, si rinvia al documento allegato n. 3 (*“Modulistica aziendale relativa all’informativa e al consenso al trattamento dei dati”*) del presente Regolamento, ove è prodotto sia il modello aziendale di **“Informativa”** che quello di raccolta del **“consenso”**, sia che ciò avvenga nei confronti di persone adulte e capaci, che di soggetti minori ed incapaci.

ARTICOLO 16. CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di **liceità del trattamento** sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal vigente Codice della privacy (*consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati*).

In particolare:

- **per i dati particolari il consenso deve essere “esplicito”** (si veda art. 9 regolamento): lo stesso dicasi per il consenso a decisioni basate su **trattamenti automatizzati** (compresa la profilazione, articolo 22);

- **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 i dati sensibili); inoltre, il Titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento;
- Il **consenso dei minori** è valido a partire dai 16 anni: prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci (articolo n. 8 del Regolamento Europeo);
- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare “caselle pre-spuntate” su un modulo);
- deve essere manifestato attraverso **“dichiarazione o azione positiva inequivocabile”** (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Interesse vitale di un terzo: si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46 del Regolamento UE).

Interesse legittimo prevalente di un titolare o di un terzo:

- Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso Titolare; si tratta di una delle principali espressioni del principio di “responsabilizzazione” introdotto dal nuovo pacchetto protezione dati;
- l'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità;
- il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

ARTICOLO 17. DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'**accesso** ai dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- f) il diritto di proporre reclamo a un'autorità di controllo;
- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- h) l'esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 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.

Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

I principi suesposti sono recepiti anche nel testo del documento allegato n. 3 (*"Modulistica aziendale relativa all'informativa e al consenso al trattamento dei dati"*) del presente Regolamento, ove è prodotto sia il modello aziendale di **"Informativa"** che quello di raccolta del **"consenso"**, sia che ciò avvenga nei confronti di persone adulte e capaci, che di soggetti minori ed incapaci.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il **diritto di accesso**, si fa rinvio alle vigenti disposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale e regionale nonché dal Garante per la privacy, con particolare riferimento all'ambito sanitario.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di **"accesso documentale"**.

A tale riguardo, si fa presente che:

- a) per **accesso documentale** si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere e provvedimenti dell'Azienda, nei termini e alle modalità previste dalla normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii. e D.P.R. 12 aprile 2006 n. 184).

Possono fare domanda tutti i cittadini portatori di un interesse *"diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso"* (art. 22, Legge 241/1990).

Per presentare domanda, è necessario rivolgersi all'Ufficio o Struttura che detiene il documento di cui si chiede l'accesso, portando con sé il proprio documento di identità valido.

I costi di ricerca, visura e riproduzione fotostatica, e le spese di spedizione, sono a carico del richiedente.

Il procedimento di accesso si conclude entro 30 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente (art. 6 del D.P.R. 184 del 2006).

Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza, che decide con provvedimento motivato, entro il termine di 20 giorni. Se l'accesso è stato negato o differito il suddetto Responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di 10 giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per

l'adozione del provvedimento da parte del Responsabile è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti 10 giorni. Avverso la decisione dell'amministrazione competente o, in caso di richiesta di riesame, avverso quella del Responsabile della Prevenzione della Corruzione e della Trasparenza, il richiedente può proporre ricorso al tribunale amministrativo regionale (TAR).

ARTICOLO 18. DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, 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.

ARTICOLO 19. DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il **diritto "all'oblio"**, che si configura come un diritto alla cancellazione dei propri 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" (si veda art. 17, paragrafo 2 del Regolamento UE).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda articolo 17, paragrafo 1).

ARTICOLO 20. DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l'interessato chiede la rettifica dei dati** (*in attesa di tale rettifica da parte del titolare*) **o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento** (*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.

ARTICOLO 21. DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste **specifiche condizioni per il suo esercizio**; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi 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 (si veda il considerando 68 del Regolamento UE).

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

ARTICOLO 22. DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, 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'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, 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.

ARTICOLO 23. PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la **profilazione**, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

PARTE QUARTA TITOLARE E RESPONSABILE DEL TRATTAMENTO

ARTICOLO 24. TITOLARE DEL TRATTAMENTO

Il **"Titolare"** del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente normativa sulla privacy, è l'Associazione Primavera Onlus, nella persona del suo Presidente, in qualità di legale rappresentante della stessa, con sede in Via Scaldamosche N. 84 a Bivona (AG).

Il Titolare, avvalendosi della supervisione e collaborazione del **Responsabile della Protezione dei Dati** aziendale, provvede:

- a) a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
- b) a nominare con atto deliberativo i *Responsabili del trattamento dei dati personali*, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy così come novellato dal D.Lgs 10/08/2018 n. 101 e all'articolo 12 del Regolamento UE 679/2016, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
- c) a nominare il Responsabile della Protezione dei Dati, come stabilito dall'articolo 37 del Regolamento UE;
- d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- e) a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla **“responsabilizzazione”** (*accountability* nell'accezione inglese) di titolari e responsabili, ovvero sulla adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del Regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto 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.

Questa Azienda, nella persona del Suo Legale rappresentante, ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* sin dalla adozione della Deliberazione del CdA del 26.03.2018 relativa alle “prime azioni” aziendali utili ad ottemperare alle previsioni legislative di matrice europea.

ARTICOLO 25. CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un *accordo interno*, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

ARTICOLO 26. RESPONSABILE INTERNO DEL TRATTAMENTO DEI DATI

Secondo il D.lgs. 196/2003 e s.m.i., s'intende per Responsabile del trattamento dei dati, *“la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione ed Organismo preposti dal Titolare al trattamento di dati personali”*.

Anche se il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile “esterno” senza contemplare espressamente la figura ed i compiti del Responsabile “interno”, questa azienda, in considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di continuare a garantire, a tutti i livelli, la più efficace applicabilità dei precetti in materia di privacy, reputa necessario continuare a designare in ambito aziendale i **Responsabili interni del trattamento dei dati personali**, conferendo l'incarico a quei dipendenti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Nell'ambito dell'Associazione Primavera Onlus, in base all'organizzazione dettata dal nuovo, vigente **Atto aziendale** vengono quindi individuati quali **Responsabili interni del trattamento dei dati personali**:

- per il trattamento della gestione amministrativa della sede di Bivona il dipendente con la responsabilità della direzione amministrativa e preposta alla sicurezza aziendale;
- per il trattamento della sede amministrativa di Palermo di Via A. Borrelli N. 4, il dipendente con funzioni di preposto alla sicurezza;
- per il trattamento della sede amministrativa di Enna di Via Duca d'Aosta N. 6, il dipendente con funzioni di responsabile amministrativo della sede;
- per il trattamento della sede amministrativa di Siracusa di Via dell'Arsenale N. 54, il dipendente con funzioni di preposto alla sicurezza;
- Per i trattamenti dell'area socio-sanitaria di Enna e Caltanissetta legate al servizio ADI, il Direttore sanitario;
- Per il trattamento legato al modulo riabilitazione neuromotoria ex art. 26, il Direttore sanitario.

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

I responsabili del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Il Responsabile interno del trattamento deve:

1. trattare i dati personali, anche sensibili, osservando le disposizioni del presente Regolamento aziendale in conformità al Reg. UE 679/2016 nonché le specifiche istruzioni impartite dal Titolare;
2. garantire che, presso la propria struttura, le persone autorizzate (incaricate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;
3. adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
4. tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;
5. mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento in conformità al Reg. UE 679/2016;
6. contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Il Responsabile per il trattamento dei dati personali, nell'espletamento della sua funzione, deve inoltre collaborare con il **Responsabile della Protezione dei Dati (RPD) aziendale**, al fine di:

a) comunicare al RPD, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 riguardanti: *l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti.*

b) utilizzare il modello aziendale di *Informativa e Consenso* approvato con il presente Regolamento, verificandone il rispetto e fornendo al RPD, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;

c) rispondere alle istanze degli interessati secondo quanto stabilito dal Codice della privacy e s.m.i. stabilendo modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;

d) contribuire a far sì che tutte le misure di sicurezza riguardanti i dati dell'Azienda siano applicate all'interno dell'Azienda stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;

e) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

L'Associazione Primavera Onlus provvederà, nella persona del Titolare del trattamento, alla **nomina dei Responsabili interni del trattamento dei dati**, dandone comunicazione personale a ciascun Responsabile all'uopo nominato.

ARTICOLO 27. RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Nell'ambito dell'azienda, sono inoltre individuati quali **Responsabili "esterni" del trattamento dei dati personali**, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con l'Associazione Primavera Onlus, trattino dati di cui è titolare l'Associazione medesima e qualora siano in possesso dei requisiti previsti dall'articolo 29, primo comma, del Codice della privacy e s.m.i. (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 29 del D.lgs. 196/2003 così come novellato dal D.Lgs del 10/08/2018 N. 101 e, in particolare, ai sensi del nuovo **articolo 28 del Regolamento Europeo 2016/679**, i Responsabili esterni hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;
- trattare i dati personali, anche di natura sensibile e giudiziaria, dei pazienti (o di altri interessati) esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con l'Associazione Primavera Onlus e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento";
- nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;
- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo (*sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati*), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso l'Associazione Primavera Onlus il Responsabile Esterno del trattamento.

La designazione del Responsabile esterno viene effettuata mediante atto di nomina sottoscritto da parte del Titolare del trattamento e controfirmato per accettazione da parte del Responsabile esterno: il documento deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Azienda.

In allegato al presente Regolamento vengono quindi prodotti il **"format aziendale" di nomina** del Responsabile del trattamento esterno con relative **istruzioni per lo svolgimento dell'incarico** (Documento allegato n. 6).

Dopo l'approvazione del presente Regolamento, l'Ufficio Privacy e Qualità dell'Associazione Primavera Onlus provvederà a trasmettere il presente Regolamento a tutte le strutture aziendali interessate.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

ARTICOLO 28. INCARICATO (AUTORIZZATO) INTERNO ED ESTERNO DEL TRATTAMENTO DEI DATI

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell'incaricato al trattamento dei dati, seppure si soffermi sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere "autorizzato" al trattamento (articoli 4 e 10 del Regolamento): il D.Lgs del 10/08/2018 N. 101 che modifica il Codice della Privacy tenendo conto di ciò, all'art. 11 lettera c) comma 2) sostituisce alla parola «dell'incaricato», «della persona autorizzata»;

Come già stabilito all'articolo 6 del presente Regolamento, al momento dell'ingresso in servizio è fornita, a cura della Ufficio Privacy e Qualità, ad ogni dipendente (*oltre che ad ogni collaboratore, consulente o titolare di borsa di studio*) che tratta dati per conto dell'azienda, una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (*o nella lettera di incarico per i summenzionati soggetti non dipendenti*), con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "**incaricati ed autorizzati al trattamento dei dati**" ai sensi del D.lgs. 196/2003 e s.m.i. e del Regolamento UE 2016/679.

Detta comunicazione conterrà anche i riferimenti per reperire il presente Regolamento sul sito internet nonché sugli appositi spazi delle sedi aziendali.

Il Regolamento, pubblicato sul sito aziendale, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

Analoghe considerazioni valgono per la figura dell'**incaricato / autorizzato esterno**: tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questa azienda, pur non essendo dipendenti e neppure titolari di incarichi conferiti dalla medesima Azienda (*quali consulenze, collaborazioni o borse di studio conferite dall'Associazione Primavera Onlus*), devono essere designati da parte del Responsabile (in questo caso "esterno") tramite una lettera (o una nota) di nomina come *incaricati esterni*.

Ci si riferisce, a titolo esemplificativo, al *personale tirocinante* o al *personale volontario* che opera temporaneamente all'interno dell'Azienda in virtù di un accordo o di una convenzione con un Ente esterno pubblico o privato (es. Associazione di volontariato o Ente universitario) per lo svolgimento, appunto, di tirocini formativi piuttosto che di attività di volontariato a sostegno degli assistiti o utenti.

Il personale di cui si parla è soggetto agli stessi obblighi cui sono sottoposti tutti gli incaricati "interni", in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Nel caso di Incaricati esterni, l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

ARTICOLO 29. RESPONSABILE AZIENDALE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del **Data Protection Officer** (in italiano: Responsabile della protezione dei dati o 'RPD'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

La nomina del RPD è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come attività principali i dati sensibili su larga scala, come ospedali, assicurazioni e istituti di credito.

Chi svolge la funzione di RPD, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in **conflitto di interessi** in quanto il Regolamento UE vieta di nominare RPD anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

Si tratta di una figura dirigenziale, di alta professionalità, a metà tra il *consulente* ed il *revisore* e non dovrebbe ricoprire ruoli gestionali rispetto all'attività dell'azienda o ai fini istituzionali della Pubblica Amministrazione.

Anche l'Associazione Primavera Onlus provvede al conferimento dell'incarico di cui si tratta, tenendo conto delle prescrizioni sin qui descritte.

Ai sensi dell'articolo 39 del Regolamento UE, i suoi compiti sono:

- **sorvegliare l'osservanza del Regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
- **fornire consulenza e pareri** al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- collaborare con il titolare, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA)**;
- **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;
- **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.
- Ai sensi dell'articolo 37 del Regolamento UE, Egli deve:
- **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
- **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse**. In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
- **operare alle dipendenze del titolare oppure sulla base di un contratto di servizio** (RPD esterno);
- **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione *on line* del curriculum del RPD, nonché la pubblicazione sul sito istituzionale dell'Ente dei "dati di contatto" del RPD: dati che debbono essere inseriti anche nell'informativa aziendale sul trattamento dei dati, così che il RPD sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la privacy.

Sia che il RPD sia interno che esterno, è necessario stipulare con il medesimo un contratto ad hoc. Nel caso il cui il RPD sia un "esterno" (persona o società) tutte le clausole, oltre che il compenso per l'incarico, dovranno essere inserite in un apposito contratto di servizi, ove siano anche previste le risorse necessarie a far funzionare l'ufficio del RPD.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

ARTICOLO 30. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio 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 del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("*sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso*", secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

ARTICOLO 31. REGISTRO ELETTRONICO DELLE ATTIVITA' DI TRATTAMENTO

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un **registro delle operazioni di trattamento** i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche 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.

Il Registro, in virtù delle dimensioni e della complessità che caratterizzano questa Azienda (che ha più di 100 dipendenti), ha forma sia cartacea che elettronica, e deve essere esibito su richiesta del Garante.

La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

Per tale motivo, anche questa azienda, per mezzo dei competenti servizi dell'Ufficio Privacy e Qualità, è impegnata a compiere i passi necessari per aggiornare tale registro elettronico.

ARTICOLO 32. PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono **“garantire un livello di sicurezza adeguato al rischio”** del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva (“tra le altre, se del caso”).

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure “minime” di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato “B” al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso

le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

ARTICOLO 33. NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

A partire dal 25 maggio 2018, tutti i titolari, e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi, dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque **“senza ingiustificato ritardo”**, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di **“Data Breach”**.

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre **“senza ingiustificato ritardo”**; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice.

I contenuti della notifica all’Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento.

Su questo e su tutta la disciplina in materia, il *Comitato europeo della protezione dati* (si veda art. 70, paragrafo 1, lettere g e h) è chiamato a formulare linee-guida specifiche, alle quali sta già lavorando il Gruppo “Articolo 29”.

Il Titolare del trattamento, sentito il RPD aziendale, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Si ricorda, inoltre, che l’Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico

(<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835>) che intende rielaborare al fine di renderlo utilizzabile da tutti i titolari di trattamento secondo quanto prevede il regolamento.

Il predetto modello è allegato al presente Regolamento (*allegato n. 8*).

ARTICOLO 34. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Le misure di sicurezza devono **“garantire un livello di sicurezza adeguato al rischio”** del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell’art. 32 è una lista aperta e non esaustiva (“tra le altre, se del caso”).

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel Regolamento UE rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento.

Quest’ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All’esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) 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’articolo 58: dall’ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

ARTICOLO 35. TRASFERIMENTO DI DATI PERSONALI ALL’ESTERO

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

ARTICOLO 36. DISCIPLINA AZIENDALE SULLA VIDEOSORVEGLIANZA

Si fa rinvio alle disposizioni di cui al *Regolamento aziendale* tempo per tempo vigente, che disciplina la materia di cui si tratta (allegato n. 9 del presente Regolamento).

ARTICOLO 37. DISCIPLINA AZIENDALE SULL’UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI

Si fa rinvio alle disposizioni di cui al *Regolamento aziendale* tempo per tempo vigente, che disciplina la materia di cui si tratta (allegato n. 10 del presente Regolamento).

PARTE SESTA

ATTUAZIONE IN AMBITO AZIENDALE DEGLI ADEMPIMENTI EUROPEI

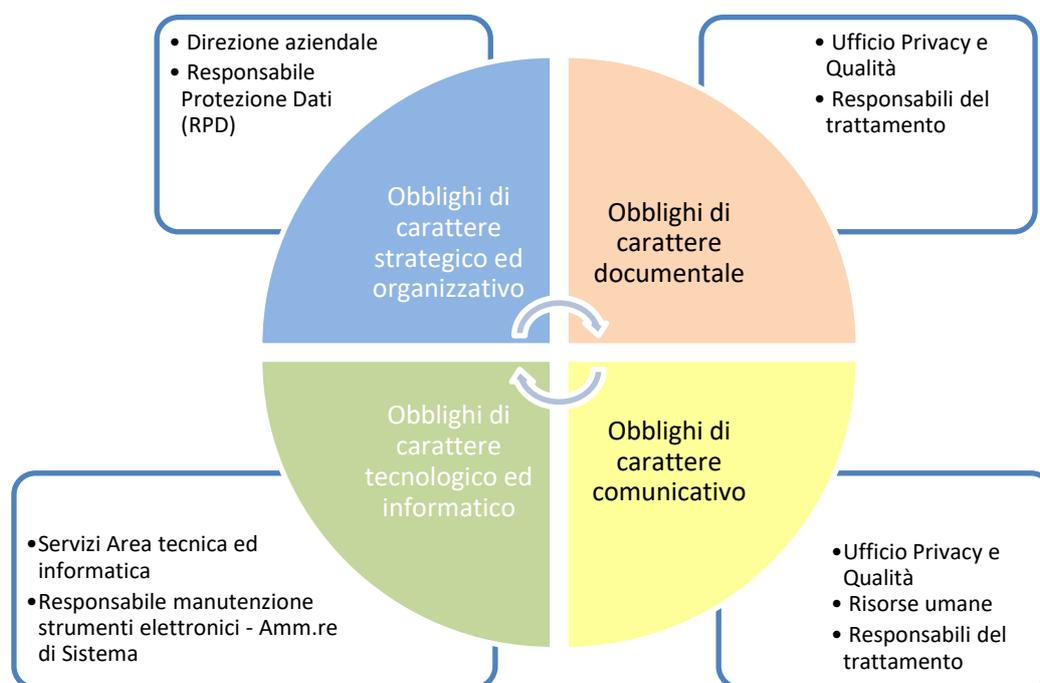
ARTICOLO 38. AMBITI DI ATTIVITÀ AZIENDALI CORRELATI AI NUOVI OBBLIGHI EUROPEI

Risultano esservi quattro tipologie di adempimenti agli obblighi europei e quindi quattro ‘macro-ambiti’ di attività aziendali ad essi collegati.

Il Regolamento europeo, infatti, detta obblighi di carattere:

- **strategico ed organizzativo**
- **documentale**
- **tecnologico ed informatico**
- **comunicativo**

Nel *grafico* che segue viene rappresentato il “ciclo di adempimenti” che questa azienda ha posto in essere, sin dal mese di marzo 2018, per realizzare la *compliance al GDPR*, individuando le strutture dell’azienda coinvolte nel medesimo ciclo:



Si dà atto che, con la Deliberazione del CdA del 26/03/2018 è stato dato avvio alle **azioni di carattere organizzativo, gestionale e documentale** volte ad ottemperare, nell’ambito dell’Associazione Primavera Onlus, agli obblighi del Regolamento Europeo, e si è provveduto ad incaricare le Strutture, i Servizi e gli Uffici coinvolti negli adempimenti di cui si tratta, come appositamente individuati nella Relazione tecnica allegata alla medesima deliberazione, affinché gli stessi pongano in essere, ciascuno secondo le rispettive competenze, ogni azione utile ad ottemperare agli obblighi europei correlati all’applicazione diretta, a far data dal 25 maggio 2018, del Regolamento anzidetto.

ARTICOLO 39. ENTRATA IN VIGORE E PUBBLICITÀ

Il presente Regolamento entrerà in vigore dalla data di adozione con atto deliberativo del CdA.

Il Regolamento verrà pubblicato sul sito internet aziendale (nell'apposita, nuova sezione dedicata alla "privacy"), nonché sugli spazi appositi delle sedi amministrative aziendali.

ARTICOLO 40. DISPOSIZIONE FINALE RELATIVA AGLI "ALLEGATI TECNICI"

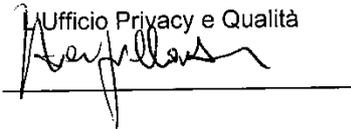
Il testo del presente Regolamento (composto di 40 articoli) potrà essere aggiornato con atto deliberativo del CdA dell'Associazione Primavera Onlus, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che europea, in materia di protezione dei dati personali.

Quanto, invece, agli **Allegati tecnici** al presente Regolamento, si stabilisce quanto segue: poiché si tratta di "strumenti di lavoro quotidiano", essi saranno inevitabilmente oggetto di continue, quanto rapide integrazioni, modifiche e revisioni, in virtù sia delle necessità aziendali che delle esigenze imposte da una realtà normativa ed organizzativa tuttora in rapidissima evoluzione.

Gli eventuali aggiornamenti ai *documenti tecnici allegati* verranno, pertanto, inseriti in tempo reale sul sito internet aziendale nell'apposita sezione dedicata alla "privacy europea", prescindendo dall'adozione di appositi atti deliberativi di modifica del presente Regolamento e dandone pubblicità per mezzo della mail "everyone", così da consentire una rapida consultazione on line dei medesimi ed un contenuto sempre aggiornato degli stessi.

Bivona, 20/09/2018

Ufficio Privacy e Qualità



Il Titolare del trattamento




Visto ed approvato: IL RPD

