REGOLAMENTO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

Matrice delle revisioni					
Revisione	Data	Descrizione / Tipo modifica	Redatta da	Verificata da	Approvata da
00	02/11/2021	Emissione	Elisa Boschetto	RPD Elena Cussigh Alessandro Camarda	Giuseppe Tonutti

Sommario

PREMESSA

La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale dell'Unione Europea. L'art. 8, par. 1 della Carta dei diritti fondamentali dell'Unione Europea, nonché l'art. 16, par. 1 del Trattato sul funzionamento dell'Unione Europea, stabiliscono, infatti, che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Il diritto alla *privacy* costituisce, 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, nonché la dignità del singolo individuo.

In attuazione di quanto sopra, il 24 maggio 2016 è entrato in vigore il Regolamento Europeo 2016/679 (GDPR), divenuto definitivamente applicabile in tutti gli Stati membri con decorrenza 25 maggio 2018.

A livello nazionale, in attuazione dell'art. 13 della l. 163/2017, il legislatore italiano ha adottato il decreto legislativo 10 agosto 2018, n. 101, a mezzo del quale ha provveduto all'abrogazione e alla modifica di tutte le disposizioni del decreto legislativo 30 giugno 2003, n. 196 incompatibili con il GDPR.

Per quanto sopra, la "cultura della *privacy*" diviene un vero e proprio elemento cardine dell'organizzazione di tutte le Pubbliche Amministrazioni.

ARCS, pertanto, si adopera affinché si rafforzi una maggiore consapevolezza della materia all'interno della propria organizzazione e ciò, non solo con la conoscenza dei principi fondamentali alla base della vigente normativa nel trattamento dei dati, ma anche ponendo in essere tutti gli adempimenti di carattere tecnico e organizzativo atti a contribuire al miglioramento della qualità del rapporto con l'utenza e il trattamento dei dati.

PARTE PRIMA: DISPOSIZIONI GENERALI

ARTICOLO 1: AMBITO DI APPLICAZIONE

Il presente regolamento disciplina, nell'ambito delle attività istituzionali attribuite dall'articolo 4 della legge regionale 27 dicembre 2018, n. 27 e ss.mm. e ii., le modalità di trattamento dei dati personali, nel rispetto di quanto previsto dalla normativa europea e nazionale.

ARTICOLO 2: FINALITÀ DEL REGOLAMENTO

L'Azienda garantisce che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, 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, dalla residenza o da altre condizioni e/o *status* personali dell'interessato.

ARTICOLO 3: PRINCIPI - *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*.

I dati personali devono essere:

- trattati in modo lecito, corretto e trasparente (liceità e trasparenza);
- raccolti per finalità determinate, esplicite e legittime e trattati compatibilmente con tali finalità (limitazione della finalità);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
- esatti e, se necessario, aggiornati (esattezza);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione);
- 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).

Il Titolare del trattamento deve rispettare i predetti principi e deve essere in grado di comprovare il rispetto degli stessi. Deve, inoltre, mettere in atto, riesaminare e aggiornare, le misure tecniche e organizzative impiegate nella realtà in cui opera, per garantire, ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR.
Unitamente a detto principio, il comportamento del Titolare deve garantire il rispetto della liceità e della trasparenza.
Quest'ultimo principio si sostanzia nell'obbligo in capo al Titolare di informare gli interessati in merito al trattamento dei loro dati personali, di rendere le informazioni richieste in caso di esercizio dei diritti e di informare gli interessati in caso di violazione dei dati personali (c.d. *data breach*).
Rispetto al principio di liceità, invece, il trattamento può dirsi in linea generale lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- 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;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- 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 richiedano la protezione dei dati personali, in particolare se l'interessato è un minore.

Il GDPR prescrive, inoltre, all'art. 25, l'obbligo del Titolare del trattamento:

- di mettere in atto misure tecniche e organizzative adeguate al fine di attuare i principi di protezione dei dati e assicurare nel trattamento le garanzie necessarie di conformità al Regolamento e di tutelare gli interessati, tutelando in tal modo il dato personale fin dalla progettazione (*privacy by design*);
- di mettere in atto misure tecniche e organizzative adeguate al fine di garantire che siano trattati secondo un'impostazione predefinita solo i dati personali necessari per ogni specifica finalità di trattamento (*privacy by default*).

ARTICOLO 4: SENSIBILIZZAZIONE

ARCS sostiene e promuove ogni strumento di sensibilizzazione al fine di consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità delle attività svolte rispetto all'utente finale.
A tale riguardo, l'Azienda promuove l'attività formativa del proprio personale e l'attività informativa diretta a tutti coloro che intrattengono rapporti con l'Azienda stessa.
Per garantire la conoscenza capillare e l'applicazione delle disposizioni introdotte dal nuovo Regolamento europeo, ARCS adotta e implementa un Modello Organizzativo Privacy (MOP), reso disponibile sul sito *web* aziendale.
Nell'ambito del MOP, tra le altre, ciascuna struttura aziendale è tenuta a dotarsi e a tenere costantemente aggiornato un Registro dei trattamenti di competenza.

ARTICOLO 5: DATI COMUNI

I dati comuni comprendono qualsiasi informazione riguardante una persona fisica identificata o identificabile, inclusi i dati sottoposti a tecniche di pseudonimizzazione.
Sono considerati a titolo meramente esemplificativo e non esaustivo: il nome e il cognome di un individuo, il numero di telefono, l'indirizzo e-mail, il codice fiscale, l'immagine fotografica di una persona, una registrazione vocale, una targa automobilistica, un indirizzo IP.
Il trattamento dei dati, a eccezione delle categorie particolari di dati personali e quelli relativi a condanne penali o reati (v. *infra* artt. 6 e 7), è consentito, e quindi lecito, se fondato su una delle seguenti basi giuridiche:

- il consenso espresso dell'interessato al trattamento;
- l'esecuzione di un contratto di cui l'interessato è parte o l'esecuzione di misure precontrattuali adottate su sua richiesta;
- l'adempimento di un obbligo legale al quale è soggetto il Titolare del trattamento;
- la necessità di salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica;
- l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

- la necessità di perseguire l'interessa legittimo del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedano la protezione dei dati personali. Nel caso in cui l'interessato è un minore, tale base giuridica non trova applicazione al trattamento dei dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

ARTICOLO 6: DATI PARTICOLARI

I dati particolari comprendono:

- i dati personali che rilevano l'origine razziale o etica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale;
- i dati genetici;
- i dati biometrici intesi a identificare in modo univoco una persona fisica;
- i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Sebbene di regola non consentito, il trattamento delle categorie particolari di dati può essere lecito al verificarsi di almeno una delle seguenti ipotesi:

- l'interessato ha prestato il proprio consenso esplicito;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare o dell'interessato in materia di diritto del lavoro o della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
- il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento è effettuato, nell'ambito delle sue legittime attività e adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contratti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria od ogniqualvolta le autorità giudiziarie esercitino le loro funzioni istituzionali;
- il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione e degli Stati membri;
- 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;
- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici sulla base del diritto dell'Unione o degli Stati membri;

- il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità con l'art. 89, par. 1 del GDPR.

ARTICOLO 7: DATI PERSONALI RELATIVI A CONDANNE PENALI O REATI

Il trattamento dei dati personali relativi a condanne penali o reati è generalmente non consentito, è da considerarsi legittimo qualora sia autorizzato da una norma di legge o di regolamento.
In particolare, ARCS può trattare dati relativi a condanne penali o reati per il perseguimento di finalità di vigilanza, di controllo o ispettiva.
Ciò premesso, a titolo esemplificativo ma non esaustivo, il trattamento può interessare:

- il diritto del lavoro, nei limiti stabiliti dalla legge, regolamenti e contratti collettivi;
- la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalla legge o dai regolamenti;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti previsti dalla legge e dai regolamenti;
- l'adempimento di obblighi previsti dalla legge in materia di prevenzione alla corruzione e di trasparenza;
- la produzione della documentazione prescritta dalla legge per la partecipazione a una procedura a evidenza pubblica;
- l'accertamento del requisito di idoneità morale di coloro che partecipano a una procedura a evidenza pubblica.

ARTICOLO 8: TRATTAMENTO IN AMBITO PUBBLICO - SISTEMA DI BILANCIAMENTO TRA RISERVATEZZA E ACCESSO

Il d.lgs. 196/2003 disciplina il rapporto tra la normativa in materia di trattamento dei dati, quella in tema di diritto di accesso ai documenti amministrativi e quella relativa all'accesso civico, sancendo l'obbligo di effettuare un bilanciamento dei diversi diritti coinvolti.
In materia di accesso e di riservatezza dei dati, il Legislatore ha provveduto a codificare una serie di principi guida, volti a consentire il summenzionato bilanciamento.
In caso di un'istanza d'accesso, è necessario svolgere un'attenta analisi del caso di specie, valutando gli interessi opposti e formulando una graduazione del diritto di accesso in relazione alla tipologia di dati personali coinvolti.
In via generale, la prevalenza del diritto di accesso deve essere garantita ai richiedenti, ogni qual volta l'istanza sia preordinata per curare o difendere i propri interessi giuridici.
Nel caso in cui l'accesso sia diretto a documenti contenenti dati particolari (*ex* art. 9 GDPR) o dati relativi a condanne o reati (*ex* art. 10 GDPR), l'accesso è consentito nei limiti in cui sia strettamente indispensabile, mentre in presenza di dati idonei a rivelare lo stato di salute e la vita sessuale (c.d. dati supersensibili o sensibilissimi), l'accesso è consentito tenuto conto dei seguenti elementi: il trattamento può verificarsi qualora la situazione giuridicamente rilavante che s'intende tutelare con la richiesta di accesso ai documenti amministrativi sia di rango almeno pari ai diritti dell'interessato ovvero consista in un diritto della personalità o libertà fondamentale (*ex* art. 60 d.lgs. 196/2003).

ARTICOLO 9: TRATTAMENTO IN AMBITO SANITARIO

I dati relativi alla salute, assieme ai dati genetici e biometrici, sono espressamente inclusi nel novero dei dati particolari e, pertanto, il trattamento di tali dati è generalmente non consentito a eccezione delle ipotesi di seguito indicate.
Preliminarmente per "dati relativi alla salute" s'intendono quei dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, idonei a rivelare informazioni relative al suo stato di salute.
Il trattamento di dati relativi alla salute è considerato lecito se:

- avviene per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei servizi sanitari o sociali (finalità di cura);
- per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

In tutti gli altri casi, il trattamento dei dati sanitari postula il consenso dell'interessato, preceduto da idonea informativa.
L'informativa deve essere concisa, trasparente, intelligibile, facilmente accessibile, scritta con linguaggio semplice e chiaro. Inoltre, tra le informazioni che devono essere fornite all'interessato, va segnalato il tempo di conservazione dei dati sanitari, definito dal Titolare stesso sulla base della finalità perseguita (v. *infra* art. 25).
I trattamenti che sono essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute e sono effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza, non richiedono il consenso al trattamento dei dati da parte dell'interessato.
Viceversa, è possibile trattare dati sanitari solo previa acquisizione del consenso nei casi di (a titolo esemplificativo e non esaustivo):

- consultazione del Fascicolo sanitario elettronico;
- consegna del referto online;
- utilizzo di app mediche.

ARTICOLO 10: TRATTAMENTO A FINI DI RICERCA SCIENTIFICA E STATISTICI

Il trattamento di dati personali a fini di ricerca scientifica e statistici è soggetto, ai sensi dell'art. 89 del GDPR, a garanzie adeguate per i diritti e le libertà dell'interessato, tali da assicurare la predisposizione di misure tecniche e organizzative atte a garantire il rispetto del principio della minimizzazione dei dati, anche a mezzo della pseudonimizzazione, purché ciò consenta di conseguire le finalità in questione.
S'intende per:

- trattamento di dati a fini statistici, qualsiasi trattamento effettuato per le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- trattamento di dati a fini scientifici, qualsiasi trattamento effettuato per le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

L'Azienda cura il trattamento dei dati, anche per dette finalità, e, nel rispetto della normativa comunitaria e nazionale, è tenuta ad adoperarsi affinché dette categorie di dati vengano sottoposte a tecniche di anonimizzazione o pseudonimizzazione.

ARTICOLO 11: COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione di dati sensibili e giudiziari da parte del Titolare è ammessa solo quando prevista da una norma di legge o di regolamento e, comunque, quando è ritenuta necessaria per lo svolgimento di prestazioni che hanno ricevuto esplicito consenso da parte dell'interessato, anche a seguito di un bilanciamento degli interessi coinvolti.
Si rinvia ai principi dettati dal GDPR (articoli 44 e ss.), nonché alle indicazioni dettate in materia, dal legislatore nazionale e dal Garante per la protezione dei dati personali.

PARTE SECONDA: DIRITTI DELL'INTERESSATO

ARTICOLO 12: DIRITTO DI ACCESSO

Il diritto di accesso, disciplinato dall'articolo 15 del GDPR, consiste nel diritto dell'interessato di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e di ottenere l'accesso ai dati personali, nonché 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, par. 1 e 4 del GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
In caso di trasferimento di dati personali verso 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 del GDPR.
Il Titolare del trattamento deve fornire una copia dei dati personali oggetto di trattamento, nel rispetto dei diritti e libertà altrui. In caso di richiesta di ulteriori copie, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.
Le informazioni sono fornite per iscritto o con altri mezzi. Se l'interessato esercita il diritto di accesso mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune. Solo se richiesto dall'interessato le informazioni sono fornite con altri mezzi purché sia possibile comprovare l'identità dell'interessato.

ARTICOLO 13: DIRITTO DI RETTIFICA

Ai sensi dell'articolo 16 del GDPR, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo, nonché l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa, tenuto conto delle finalità del trattamento.
Inoltre, secondo le disposizioni dell'art. 19 del GDPR, il Titolare deve comunicare ai destinatari a cui sono stati trasmessi i dati personali, le eventuali rettifiche del trattamento salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato e, comunica all'interessato tali destinatari qualora richiesto da quest'ultimo.

ARTICOLO 14: DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

L'articolo 17 del GDPR dispone che l'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei suoi dati personali senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.
Tale diritto può essere esercitato dall'interessato se sussiste uno dei seguenti motivi:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento conformemente all'art. 6, par. 1, lett. a), o all'art. 9, par. 2, lett. a), e se non sussiste altro formato giuridico per il trattamento;
- l'interessato si oppone al trattamento ai sensi dell'art. 21, par. 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'art. 21, par. 2;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione europea o dello Stato membro cui è soggetti il Titolare del trattamento;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art. 8, par. 1.

Il Titolare deve comunicare ai destinatari a cui sono stati trasmessi i dati personali le eventuali cancellazioni del trattamento, salvo che ciò riveli impossibile o implichi uno sforzo sproporzionato, e se l'interessato lo richiede gli comunica tali destinatari.
Nel caso in cui il Titolare abbia reso pubblici i dati, lo stesso deve altresì adottare le misure tecnologiche, anche tecniche, per informare i Titolari del trattamento che stanno trattando i dati personali in merito alla richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali.
In ogni caso, il diritto di cancellazione non può essere esercitato se necessario per:

- l'esercizio del diritto alla libertà di espressione e di informazione;
- l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione europea e dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interessate oppure nell'esercizio di pubblici poteri di cui è investito il Titolare;
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'art. 9, par. 2, lett h) e i), e dell'art. 9, par. 3;
- fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

ARTICOLO 15: DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Ai sensi dell'art. 18 del GDPR, il diritto di limitazione di trattamento ricorre in una delle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati e chiede, invece, che ne sia limitato l'utilizzo;
- i dati personali, non più necessari per il Titolare, diventano indispensabili per l'accertamento, l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria;
- l'interessato si è opposto al trattamento ai sensi dell'art. 21, par. 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare.

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione non è consentito a meno che ricorrano determinate circostanze (a titolo esemplificativo: consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

ARTICOLO 16: DIRITTO ALLA PORTABILITÀ DEI DATI

Ai sensi dell'art. 20 del GDPR, il diritto alla portabilità si raffigura nel diritto di:

- ricevere in un formato strutturato i dati personali che lo riguardano forniti a un Titolare;
- trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del Titolare al trattamento cui li ha forniti qualora il trattamento si basi sul consenso o su un contratto; e il trattamento sia effettuato con mezzi automatizzati.

L'interessato ha comunque il diritto a ottenere che la trasmissione dei dati personali da un titolare del trattamento all'altro avvenga direttamente, se tecnicamente fattibile, fermo restando il diritto alla cancellazione.
Tale diritto, infine, non trova applicazione nel caso di trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare.

ARTICOLO 17: DIRITTO DI OPPOSIZIONE

Come stabilito all'articolo 21 del GDPR, 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, par. 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.
Il Titolare del trattamento deve astenersi 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.
L'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
Nel caso in cui i dati personali siano trattati a fini di ricerca scientifica, storica o statistica ai sensi dell'art. 89, par. 1, l'interessato, per motivi, connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati particolari che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.
Inoltre, ai sensi dell'art. 22 del Regolamento, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione.

ARTICOLO 18: PROCEDURA PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

I soggetti cui si riferiscono i dati personali hanno il diritto di esercitare i diritti summenzionati mediante l'utilizzo di apposita modulistica "Modello Esercizio Diritti dell'interessato" resa disponibile dall'Azienda sul proprio sito *web* istituzionale ovvero attraverso il Responsabile per la Protezione dei Dati (RPD).

PARTE TERZA: I SOGGETTI E IL MODELLO ORGANIZZATIVO PRIVACY (MOP)

ARTICOLO 19: TITOLARE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento è definito all'art. 4 del GDPR 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"* e *"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"*.
Il Titolare del trattamento dei dati, ai sensi e per gli effetti della normativa in materia di *privacy*, è l'Azienda Regionale di Coordinamento per la Salute (ARCS), nella persona del suo Direttore generale, in qualità di Legale Rappresentate *pro tempore* dell'Azienda medesima.
Il Titolare deve mantenere un approccio proattivo, atto a valutare costantemente il contesto e il settore in cui opera e deve operare nel rispetto degli obblighi generali impartiti agli artt. 24 e 25 del GDPR.
Il Titolare è, altresì, il soggetto su cui grava la responsabilità generale del trattamento nonché di esatto adempimento alle prescrizioni contenute nel GDPR ed è tenuto a mettere in atto tutte le misure tecniche e organizzative adeguate al fine di dimostrare che il trattamento dei dati personali è effettuato conformemente al regolamento secondo il principio di responsabilità (c.d. "*accountabilty*"), ivi inclusa l'efficacia delle misure adottate.
A tal fine ARCS, facendo proprio il principio di *accountability,* implementa un Modello Organizzativo Privacy (MOP), finalizzato ad analizzare tutte le attività di trattamento dei dati e a organizzare le stesse all'interno delle singole strutture aziendali in modo funzionale e con l'obiettivo di gestire i dati in sicurezza e trasparenza, sempre nel rispetto dei diritti e delle libertà fondamentali di tutti gli interessati.

ARTICOLO 20: RSPONSABILE DEL TRATTAMENTO DATI *EX* ART. 28 GDPR

L'art. 28 del GDPR disciplina la figura del Responsabile del trattamento dati, a cui compete una serie di responsabilità e obblighi.
È fondamentale che ogni struttura sia in grado di distinguere i casi in cui ARCS tratta dati per conto di terzi o viceversa qualora siano i terzi a trattare dati per conto di ARCS.
In entrambe le situazioni, la struttura interessata deve rilasciare apposita nomina a Responsabile *ex* art. 28 GDPR, come da modello aziendale approvato con provvedimento del Direttore Generale.
Nel caso in cui ARCS, in qualità di Responsabile, affidi l'attività in *outsourcing* a un terzo, tra l'Azienda e quest'ultimo deve essere predisposta una nomina a sub-responsabile.
Il Responsabile *ex* art. 28 deve sempre effettuare il trattamento dei dati attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al periodo precedente e delle proprie istruzioni.

ARTICOLO 21: RESPONSABILE PER LA PROTEZIONE DEI DATI (RPD)

ARCS attua in concreto i principi di cui all'art. 3 attraverso il MOP, che si ricomprende di tutte le misure fisiche, tecniche (informative) e organizzative (procedurali) finalizzate alla prevenzione dei rischi derivanti dall'attività di trattamento.
L'Azienda è tenuta a nominare un Responsabile della Protezione Dati (RPD), il cui ruolo è quello di supportare il Titolare e tutti i dipendenti informandoli e fornendo consulenza in merito agli obblighi derivanti dal Regolamento e dalle altre disposizioni relative al trattamento, nonché sorvegliando sull'esatta applicazione degli stessi anche attraverso l'attività di formazione.

Svolge, in piena autonomia e indipendenza, i compiti e le funzioni previsti dal Regolamento UE/2016/679 e rappresenta il punto di contatto con il Garante per la protezione dei dati personali.
I dati di contattato del DPO sono pubblicati sul sito istituzionale aziendale, nonché comunicati all'Autorità di controllo, a cura del Titolare o del Responsabile del trattamento.

ARTICOLO 22: INCARICATI DI PRIMO E SECONDO LIVELLO

Ai sensi dell'art. 32 del GDPR, tra le misure organizzative cui l'Azienda è tenuta, sono ricompresi gli atti di nomina *ex* art. 29 GDPR, secondo cui *"chiunque agisca sotto l'autorità del Titolare del trattamento che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli stati membri".*
Detta normativa, unitamente al Codice Privacy (art. 2-*quaterdecies*), ripone in capo al Titolare del trattamento l'obbligo di autorizzare i propri dipendenti o collaboratori a trattare i dati dando idonee istruzioni in merito.
In applicazione di quanto sopra, ARCS individua due categorie di soggetti incaricati autorizzati al trattamento dei dati:

- incaricato di primo livello, ovvero i Responsabili preposti alla Struttura Complessa e di Struttura Semplice Dipartimentale titolari e *ad interim* di riferimento come da organigramma aziendale;
- incaricati di secondo livello, ovvero tutti i soggetti incardinati presso la Struttura Complessa o la Struttura Semplice Dipartimentale -anche in virtù del contratto di lavoro in essere- e autorizzati al trattamento dei dati personali effettuati sia con strumenti manuali che con strumenti elettronici, con accesso ai dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati.

Ciascun dipendente e collaboratore del Titolare è autorizzato a trattare solamente i dati indispensabili per svolgere le proprie mansioni, in funzione dell'organizzazione interna e per le finalità indicate all'interessato (v. sopra art. 3, principio di "limitazione della finalità e minimizzazione dei dati").

ARTICOLO 23: REFRENTE AZIENDALE

Il Referente *privacy* aziendale è individuato dal Direttore Generale tra i dirigenti amministrativi in servizio.
Il Referente *privacy* propone il regolamento aziendale *privacy* e le eventuali modifiche; fornisce supporto in materia di trattamento dati al Titolare e alle altre strutture aziendali; predispone i provvedimenti in materia di trattamento dati.

ARTICOLO 24: AMMINISTRATORI DI SISTEMA (INTERNI ED ESTERNI)

Il Titolare utilizza sistemi informatici per gestire e organizzare la propria attività. Per tale ragione da sempre l'attenzione alla costruzione dei *software* e l'utilizzo e sicurezza dei dati sono alla base dell'attività prevalente del Titolare. Con decreto del Direttore Generale di ARCS sono individuati i soggetti con privilegi di "Amministratore" interni all'Azienda e viene approvata la relativa *policy* a cui gli stessi sono tenuti ad adeguarsi; è, inoltre, predisposto un elenco degli Amministratori con indicazione delle funzioni a essi attribuite e reso disponibile a tutti i dipendenti.
Anche le altre società esterne specializzate che accedono ai dati aziendali devono essere specificatamente nominate Responsabili ai sensi dell'art. 28 del GDPR.
I fornitori di Servizi informatici esterni sono scelti con particolare attenzione alla professionalità non solo tecnica, ma anche del rispetto e della protezione dei dati, privilegiando società certificate ISO 27001.

ARTICOLO 25: CONSENSO AL TRATTAMENTO DEL DATI

La liceità del trattamento dei dati personali dipende dalla tipologia di dati trattati e delle relative modalità del trattamento. Ai sensi dell'art. 6 del GDPR il trattamento dei dati personali, come già riportato, che non appartengono a categorie particolari e che non riguardano condanne penali e reati, è consentito, quindi lecito, se sussiste una delle seguenti basi giuridiche:

- il consenso espresso dell'interessato al trattamento;
- l'esecuzione di un contratto di cui l'interessato è parte o l'esecuzione di misure precontrattuali adottate su sua richiesta;
- l'adempimento di un obbligo legale al quale è soggetto il Titolare del trattamento;
- la necessità di salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica;
- l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- la necessità di perseguire l'interesse legittimo del Titolare del trattamento di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (c.d. *balancing test*).

Per poter essere valido, quindi lecito, il consenso deve essere espresso mediante un atto positivo, libero, specifico, informato e inequivocabile dell'interessato e da cui risulti l'indubbia volontà di accettare il trattamento dei dati personali.
Il consenso può essere revocato in qualsiasi momento, senza che ciò pregiudichi la liceità del trattamento basata sul consenso prima della revoca. Il Titolare deve, altresì, essere sempre in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

ARTICOLO 26: INFORMATIVA

L'informativa è una comunicazione rivolta all'interessato da parte del Titolare del trattamento, con lo scopo di informarlo sulle finalità e le modalità dei trattamenti dati.
Essa rappresenta espressione del dovere del Titolare del trattamento di assicurare la trasparenza e la correttezza del trattamento fin dalla sua progettazione, secondo il principio di *accountability* (v. sopra art. 3).
L'informativa ha, altresì, lo scopo di porre l'interessato nella condizione di rendere un valido consenso, se richiesto come base giuridica del trattamento. In questo caso l'informativa non è solo dovuta in base al principio di trasparenza e correttezza, ma è anche una condizione di legittimità del consenso stesso.
L'informativa è dovuta, pertanto, ogni qual volta vi sia un trattamento di dati, fatta eccezione per i seguenti casi:

- la persona fisica che effettua il trattamento dei dati per attività a carattere esclusivamente personale e domestico;
- l'interessato dispone già delle informazioni;
- comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
- l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare;
- i dati personali debbano rimanere riservati per obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri;
- i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

- il trattamento è connesso allo svolgimento delle investigazioni difensive in materia penale o alla difesa di un diritto in sede giudiziaria (a meno che il trattamento si protragga per un periodo superiore a quello strettamente necessario al perseguimento di tali finalità o sia svolto per ulteriori scopi).

L'informativa, resa del tutto gratuitamente, deve, inoltre, avvenire nel rispetto dei seguenti principi:

- in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro;
- per iscritto o con altri mezzi idonei (es. posta elettronica);
- se richiesto dall'interessato anche oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

L'informativa deve avere il seguente contenuto minimo:

- l'indicazione delle categorie di dati trattati e della finalità del trattamento (quali dati vengono trattati divisi per categorie, a quale fine, per quanto tempo sono trattati, se i dati verranno trasferiti all'estero e, in questo caso, attraverso quali strumenti);
- la base giuridica del trattamento, quindi se si tratta di trattamento basato su consenso o giustificato da leggi, legittimi interessi (in questo caso specificando il legittimo interesse);
- la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di tale rifiuto;
- se il Titolare ha intenzione di utilizzare i dati per una finalità ulteriori da quelle per la quale sono stati raccolti;
- i soggetti destinatari ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi (l'indicazione di soggetti terzi non può essere generica);
- se il titolare ha intenzione di trasferire i dati in paesi *extra* UE, nel qual caso se esiste o meno una decisione di adeguatezza della Commissione UE;
- il periodo di conservazione dei dati oppure l'indicazione dei criteri per determinarlo;
- i diritti dell'interessato;
- i dati identificativi e di recapito del Titolare del trattamento e del Responsabile per la Protezione dei Dati (RPD);
- se il trattamento comporta processi decisionali automatizzati (es. di profilazione) deve essere specificato indicando anche la logica di tali processi decisionali e le conseguenze previste per l'interessato;
- se i dati sono raccolti presso terze parti, l'informativa deve presentare dei contenuti ulteriori, ovvero l'indicazione delle categorie dei dati personali oggetto del trattamento, nonché la fonte da cui hanno origine i dati personali. Nel caso di specie, va omessa l'informazione circa la natura obbligatoria o meno della comunicazione di dati personali (nella fattispecie i dati non sono raccolti presso l'interessato).

L'informativa può essere resa anche a mezzo di pubblicazione della stessa sul sito istituzionale. Ciascuna struttura aziendale è dotata -a seconda delle attività di trattamento che svolge- di idonee informative e della modulistica necessaria da rendere disponibile agli interessati. Ciascun dipendente deve essere in grado di gestire autonomamente tutta la modulistica e le informative predisposte e di conoscere il momento esatto in cui utilizzarle. A tale fine l'Azienda, attraverso *audit* interni e corsi formativi dedicati, forma i propri collaboratori affinché l'espletamento delle proprie attività avvenga sempre nel rispetto dei principi del Regolamento UE/2016/679.

ARTICOLO 27: PROCEDURA VIOLAZIONE DATI

La violazione dei dati rappresenta una violazione di sicurezza che, accidentalmente o in modo illecito, determina la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Al verificarsi di detta circostanza, ciascun incaricato di primo ovvero di secondo livello dell'Azienda deve coinvolgere immediatamente il Responsabile della struttura, il Referente *privacy*, il Responsabile Servizi Informativi e il RPD al fine di una corretta classificazione e gestione dell'evento.
La segnalazione deve avvenire a mezzo del modulo reperibile sul sito istituzionale alla voce "*data breach*" e indicata nel registro delle violazioni.
Con il supporto di soggetti suindicati, il Titolare valuta le azioni da porre in essere per limitare gli eventuali danni, i soggetti che devono agire per contenere la violazione, la necessità o meno di notificare la violazione al Garante, nonché la necessità o meno di comunicarlo anche agli interessati.

ARTICOLO 28: VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Ai sensi dell'articolo 35 del Regolamento UE/2016/679, la valutazione di impatto è una proceduta che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità, nonché i relativi rischi, allo scopo di programmare misure idonee ad affrontarli. Per questo motivo, la valutazione deve essere condotta prima del trattamento e riesaminata con regolarità.
La DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.
Sotto il profilo della responsabilizzazione (c.d. *accountability*), la DPIA aiuta il Titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni.
In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, la DPIA è necessaria in presenza di almeno due dei seguenti criteri:

- 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;
- 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;
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Sono esclusi dalla DPIA, tutti quei trattamenti che:

- non comportano un rischio elevato per i diritti e le libertà dell'interessato;
- sono assimilabili per natura, finalità e contesto ad altri trattamenti per cui sia già stata svolta una DPIA;
- sono stati sottoposti a verifica del Garante prima del maggio 2018 e non hanno subito modifiche;

- trovano base legale nel diritto della UE o dello stato membro;
- sono ricompresi nell'elenco facoltativo che verrà redatto dal Garante nel corso del tempo.

ARTICOLO 29: REGISTRO TRATTAMENTO DATI

Ciascuna struttura aziendale è tenuta a dotarsi di un registro dei trattamenti quale strumento dinamico predisposto e implementato a seconda delle esigenze, che preveda un'attenta e costante analisi dei rischi per il trattamento dei dati personali, individuati per ciascuna attività o servizio erogato.
È compito di ciascun Responsabile di struttura provvedere alla conservazione, aggiornamento e implementazione del registro relativo alla struttura cui è preposto.
L'Azienda, infine, è tenuta a dotarsi di un Registro generale di carattere più statico al cui interno sono elencate tutte le attività di trattamento e le misure di sicurezza fisiche ed organizzative comuni a tutte le strutture.

ARTICOLO 30: MISURE FISICHE, LOGISTICHE, TECNICO INFROMATICHE E CORSI DI FORMAZIONE

Il Regolamento UE/2016/679 prevede un obbligo di formazione in capo a tutte le pubbliche amministrazioni in tema di trattamento di dati personali.
In ottemperanza al dettato normativo, ARCS eroga periodicamente corsi di formazione e aggiornamento in materia, atti a sensibilizzare i propri dipendenti e collaboratori al rispetto di tutte le misure fisiche, logistiche e tecniche informatiche.
Per quanto concerne quest'ultimo settore, l'analisi sui rischi informatici e sulle infrastrutture *hardware* e *software* aziendali e sulle misure informatiche di adeguamento viene realizzata da Amministratori di sistema aziendali con appositi *tool e check list*, nonché da professionisti esterni specializzati. Gli esiti dell'indagine consentono ai tecnici aziendali di migliorare ulteriormente le misure di protezione dai *cyber* attacchi e dalle minacce informatiche, gradatamente e proporzionalmente al rischio per i diritti e le libertà degli interessati. Ogni dipendente e collaboratore è tenuto al rispetto della regolamentazione aziendale in tema di utilizzo degli strumenti informatici, nonché di comportamento, anche etico, relativamente a tutte le informazioni alle quali accede in virtù della specifica mansione.
Infine, si ricorda, che tutte le misure -organizzative, fisiche, giuridiche, tecniche ed informatiche- programmate e attuate per abbattere i rischi *privacy* dell'interessato sono previste nell'apposita sezione del registro dei trattamenti.

PARTE QUARTA: DISPOSIZIONI FINALI

ARTICOLO 31: ENTRATA IN VIGORE E PUBBLICITÀ

Il presente Regolamento entra in vigore dalla data di esecutività del Decreto del Direttore Generale di ARCS e, nel rispetto degli obblighi di trasparenza, lo stesso verrà pubblico sul sito istituzione di ARCS.

ARTICOLO 32: RINVIO AL SITO *WEB* AZIENDALE

Per la consultazione dei modelli/documenti citati nel testo del presente Regolamento, si fa espresso e integrale rinvio alla sezione dedicata alla "*Policy in materia di protezione dei dati personali*" contenuta nel sito *web* aziendale, all'interno della quale è pubblicata e tenuta costantemente aggiornata tutta la documentazione relativa alla materia.