



Repubblica Italiana
Assemblea Regionale Siciliana

**Regolamento relativo alla protezione delle
persone fisiche con riguardo al trattamento dei
dati personali nella disponibilità
dall'Amministrazione
dell'Assemblea regionale siciliana,
nonché alla libera circolazione di tali dati**

(Reso esecutivo con D.P.A. n. 406 del 20 novembre 2018)

Articolo 1 OGGETTO

1. Il presente Regolamento, in attuazione del “Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)”, e delle disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679, disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali nella disponibilità dall'Amministrazione dell'Assemblea regionale siciliana, di seguito “Assemblea” o “Titolare del trattamento”, nonché alla libera circolazione di tali dati.

2. L'Autorità di controllo di cui all'articolo 51 del Regolamento (UE) 2016/679 è individuata nel Garante per la protezione dei dati personali, di seguito “Garante”, di cui all'articolo 153 decreto legislativo 30 giugno 2003, n.196, e successive modifiche ed integrazioni.

Articolo 2 TITOLARE DEL TRATTAMENTO

1. Titolare del trattamento è l'Assemblea regionale siciliana.

Articolo 3 AMBITO DI APPLICAZIONE MATERIALE

1. Il presente Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti negli archivi dell'Assemblea regionale siciliana o destinati a figurarvi.

2. In ragione dell'autonomia costituzionalmente riconosciuta all'Assemblea regionale siciliana sono esclusi dall'applicazione della normativa di cui al comma 1 i trattamenti di dati personali effettuati in relazione all'esercizio delle funzioni parlamentari da parte degli Organi dell'Assemblea regionale siciliana.

Articolo 4 DEFINIZIONI

Ai fini del presente Regolamento si intende per:

- **“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;

- **“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;

- **“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;

- **“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;
- **“minimizzazione”**: limitazione delle operazioni di trattamento a quanto effettivamente necessario per il perseguimento delle finalità del Titolare;
- **“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;
- **“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;
- **“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;
- **“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.

Articolo 5

PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

1. 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 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) 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»);
- e) 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- f) 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»).

2. L'Assemblea regionale siciliana è competente per il rispetto del comma 1 ed è in grado di provarlo («responsabilizzazione»).

Articolo 6

LICEITA' DEL TRATTAMENTO

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
 - a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
 - b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
 - c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
 - d) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
 - e) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
2. La lettera e) del primo comma non si applica al trattamento di dati effettuato dall'Assemblea regionale siciliana nell'esecuzione delle funzioni parlamentari da parte dei suoi Organi.
3. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo che costituisca una misura necessaria e proporzionata al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, l'Assemblea tiene conto, tra l'altro:
 - a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
 - b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
 - c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali, oppure se siano trattati dati relativi a condanne penali e a reati;
 - d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
 - e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 7

CONDIZIONI PER IL CONSENSO

1. Qualora il trattamento sia basato sul consenso, l'Assemblea deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 8

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

1. 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.

2. Il comma 1 non si applica se si verifica uno dei seguenti casi:

- a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- d) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- f) il trattamento è necessario per motivi di interesse pubblico rilevante che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- g) 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 o conformemente al contratto con un professionista della sanità;
- h) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica.

Articolo 9

TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

1. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o, se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri, deve prevedere garanzie appropriate per i diritti e le libertà degli interessati.

Articolo 10

TRATTAMENTO CHE NON RICHIEDE L'IDENTIFICAZIONE

1. Se le finalità per cui l'Assemblea tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.

Articolo 11

INFORMAZIONI, COMUNICAZIONI E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

1. L'Assemblea adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative alle richieste di informazione e accesso, comprese quelle finalizzate all'esercizio del diritto di rettifica, di cancellazione e di differimento di utilizzo dei propri dati personali, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2. L'Assemblea fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli 13 e seguenti senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. L'Assemblea informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

3. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

4. Se non ottempera alla richiesta dell'interessato, l'Assemblea informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo al Garante per la protezione dei dati personali e di proporre ricorso giurisdizionale.

5. Le informazioni fornite sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

- a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta;
- b) oppure rifiutare di soddisfare la richiesta.

6. Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

7. Qualora l'Assemblea nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

Articolo 12

INFORMAZIONI DA FORNIRE ALL'INTERESSATO IN CASO DI RACCOLTA DATI

1. L'Assemblea, in caso di raccolta di dati 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, ove applicabile;
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) gli eventuali legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.

2. Qualora l'Assemblea 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 e ogni ulteriore informazione.

3. I commi 1 e 2 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 13

DIRITTO DI ACCESSO DELL'INTERESSATO

1. L'interessato ha il diritto di ottenere dall'Assemblea 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 al Garante per la protezione dei dati personali;
 - 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.
2. L'Assemblea fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, l'Assemblea 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.
3. Il diritto di ottenere una copia di cui al comma 2 non deve ledere i diritti e le libertà altrui.

Articolo 14

DIRITTO DI RETTIFICA

1. L'interessato ha il diritto di ottenere dall'Assemblea 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 15

DIRITTO ALLA CANCELLAZIONE («DIRITTO ALL'OBLIO»)

1. L'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e l'Assemblea ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
 - b) l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
 - c) l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
 - d) i dati personali sono stati trattati illecitamente;
 - e) i dati personali devono essere cancellati per adempiere un obbligo legale.
2. L'Assemblea, se ha reso pubblici dati personali ed è obbligata, ai sensi del comma 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i delegati del trattamento, che stanno trattando i dati personali, della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I commi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
- a) per l'esercizio del diritto alla libertà di espressione e di informazione;

- b) per l'adempimento di un obbligo legale che richieda il trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investita l'Assemblea;
- c) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui il diritto di cui al comma 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- d) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Articolo 16

DIRITTO DI LIMITAZIONE DI TRATTAMENTO

1. L'interessato ha il diritto di ottenere dall'Assemblea la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
 - a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
 - b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
 - c) benché l'Assemblea non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
 - d) l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi dell'Assemblea rispetto a quelli dell'interessato.
2. Se il trattamento è limitato a norma del comma 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico.
3. L'interessato che ha ottenuto la limitazione del trattamento a norma del comma 1 è informato prima che detta limitazione sia revocata.

Articolo 17

OBBLIGO DI NOTIFICA IN CASO DI RETTIFICA O CANCELLAZIONE DEI DATI PERSONALI O LIMITAZIONE DEL TRATTAMENTO

1. L'Assemblea comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. L'Assemblea comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Articolo 18

DIRITTO DI OPPOSIZIONE

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.
2. L'Assemblea si astiene dal trattare ulteriormente i dati personali salvo che 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.
3. Il diritto di cui al comma 1 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
4. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al

trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Articolo 19

PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE, COMPRESA LA PROFILAZIONE

1. 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.
2. Il comma 1 non si applica nel caso in cui la decisione:
 - a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e l'Assemblea;
 - b) sia autorizzata dal diritto dell'Unione o dello Stato italiano, che precisa, altresì, misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
 - c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al comma 2, lettere a) e c), l'Assemblea attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Articolo 20

RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, l'Assemblea mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Le misure di cui al comma 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati.

Articolo 21

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

1. Tenendo conto della propria organizzazione giuridica e tecnologica e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, l'Assemblea mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. L'Assemblea, inoltre, mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Articolo 22

DELEGATI AL TRATTAMENTO

1. In considerazione della complessità e delle molteplicità delle funzioni istituzionali svolte dall'Assemblea, in cui le scelte di gestione amministrativa, tecnica e finanziaria rientrano tra le specifiche competenze attribuite ai Direttori di Servizio, al Capo di Gabinetto ed ai titolari di Incarico speciale, tali Soggetti, nonché gli altri eventualmente individuati dal Segretario generale con proprio provvedimento, sono delegati, ognuno per il proprio ambito di competenza, al trattamento dei dati personali effettuato nello svolgimento delle proprie attribuzioni.

2. Ai delegati al trattamento di cui al comma 1, sono attribuiti i compiti di:

- a) osservare i principi applicabili al trattamento dei dati personali e le condizioni di liceità del trattamento; garantire la qualità dei dati personali, le corrette modalità di raccolta, conservazione e trattamento degli stessi, anche da parte del personale autorizzato della propria struttura e da eventuali responsabili del trattamento che saranno dagli stessi individuati e designati, secondo quanto disposto dal Regolamento e vigilare sul rispetto delle istruzioni impartite;
- b) tenere traccia del percorso logico e delle motivazioni che hanno condotto ad effettuare le scelte in ambito privacy;
- c) fornire le informative agli interessati;
- d) implementare, con le informazioni relative alla struttura di competenza, il Registro (unico) delle attività di trattamento, conformemente alle istruzioni ricevute al momento dell'avvio del Registro;
- e) curare l'adozione delle misure di sicurezza adeguate, con particolare riguardo ai trattamenti effettuati senza l'ausilio di mezzi elettronici;
- f) coinvolgere tempestivamente e adeguatamente, in tutte le questioni riguardanti la protezione dei dati personali, anche per il tramite dei referenti, il Responsabile per la protezione dei dati e collaborare con il medesimo per ogni questione relativa al trattamento dei dati, consentendo altresì verifiche privacy presso la propria struttura;
- g) autorizzare al trattamento i dipendenti della propria struttura che trattano dati personali, individuandoli quali "*persone autorizzate al trattamento*" e verificare che questi trattino i dati personali strettamente indispensabili per lo svolgimento delle attività loro assegnate, nel rispetto dei principi applicabili.

Articolo 23

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

1. L'Assemblea tiene un registro in formato elettronico delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

- a) il nome e i dati di contatto del Titolare del trattamento, del Delegato al trattamento e del Responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati.

Articolo 24

SICUREZZA DEL TRATTAMENTO

1. Tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, nonché dei costi di attuazione, l'Assemblea mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la minimizzazione;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
 3. L'Assemblea assicura che chiunque agisce sotto la sua autorità e ha accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso.

Articolo 25

DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

1. L'Assemblea, con decreto del Presidente dell'Assemblea, designa il Responsabile della protezione dei dati.
2. Il Responsabile della protezione dei dati:
 - è scelto tra i Consiglieri parlamentari dell'Assemblea almeno alla seconda fascia stipendiale;
 - non deve trovarsi in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare;
 - è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti e deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
3. Al Responsabile della protezione dati sono attribuiti i compiti di:
 - a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
 - b) sorvegliare l'osservanza del presente Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
 - c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
 - d) cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
4. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
5. Il nominativo e i dati di contatto del Responsabile per la protezione dei dati sono comunicati al Garante per la protezione dei dati personali e i dati di contatto sono pubblicati sul sito internet dell'Assemblea regionale siciliana.

Articolo 26

VIOLAZIONE DI DATI PERSONALI – DATABREACH

1. In caso di violazione dei dati personali, che comporti 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, l'Assemblea ha l'obbligo di notificare la violazione al

Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

2. La notificazione al Garante è subordinata alla valutazione del rischio per gli interessati che spetta al titolare del trattamento.

3. La notifica di cui al comma 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le stesse possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. L'Assemblea documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente al Garante di verificare il rispetto del presente articolo.

Articolo 27

COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al comma 1 descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo precedente, comma 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al comma 1 se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al comma 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analogo efficacia.

4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante per la protezione dei dati personali può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al comma 3 è soddisfatta.

Articolo 28

TUTELA DELL'INTERESSATO E SANZIONI

1. Per la tutela dei diritti dell'interessato e l'applicazione di eventuali sanzioni, si applica la Parte Terza del decreto legislativo 30 giugno 2003, n.196, e successive modifiche ed integrazioni.

Articolo 29

DISPOSIZIONI FINALI

1. Per quanto non espressamente previsto dal presente Regolamento si applicano le norme del *Regolamento UE 27 aprile 2016 n. 679 del Parlamento europeo e del Consiglio del 27 aprile 2016* e le disposizioni per l'adeguamento della normativa nazionale applicabili alle Istituzioni Pubbliche.

M