DISPOSIZIONI
per il trattamento dei dati personali

Istruzioni e misure organizzative e
Tecniche

Premessa

Il Parlamento Europeo ed il Consiglio hanno approvato, nella seduta del 27 aprile 2016, il Regolamento 2016/679/UE (noto anche come "GDPR – *General Data Protection Regulation*") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati. Detto Regolamento, che abroga la Direttiva 1995/46/CE si applica, senza necessità di recepimento, in tutti gli Stati membri dell'Unione Europea a far data dal 25 maggio 2018.
Con la nuova normativa europea la protezione dei dati personali cambia profondamente, in particolare per effetto dell'introduzione del principio della "responsabilizzazione" ("*accountability*"), che attribuisce al Titolare del trattamento il compito di mettere in atto "*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento*". Il presente documento intende pertanto fornire prime istruzioni e direttive per i trattamenti di dati personali effettuati da Strutture della Giunta Regionale della Campania, senza per questo assumere esaustività rispetto alle previsioni del Regolamento 2016/679, che pertanto deve essere conosciuto e rispettato in tutte le sue parti da tutti coloro che, a qualsiasi titolo, trattano dati personali.
Il presente documento, inoltre, deve considerarsi integrato dalle eventuali indicazioni e linee guida che saranno emanate dall'Autorità italiana Garante della Privacy nonché dalle ulteriori disposizioni che il legislatore italiano dovesse adottare, nei limiti dello spazio di discrezionalità lasciato ai singoli stati membri del cennato Regolamento.

PARTE PRIMA
Inquadramento generale

1. Definizioni e principi applicabili al trattamento dei dati personali

L'articolo 4 del Regolamento 2016/679/UE fornisce alcune **definizioni**, le cui principali si riportano di seguito:

1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente 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;
5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che

tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
16) «**stabilimento principale**»:
a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
[…]

18) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
[…]
21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Si può osservare in primo luogo dall'esame delle definizioni contenute nell'articolo 4 del *Regolamento* che, nella nuova disciplina, non compaiono più, rispetto al D. Lgs. 196/2003, le definizioni di Incaricato, dati sensibili, dati giudiziari e dati anonimi.
Tuttavia, a proposito degli Incaricati, al punto n. 10 del citato articolo 4, nel fornire la definizione di "terzo" si fa un accenno a "*persone autorizzate al trattamento*", concetto assimilabile a quello della precedente figura dell'incaricato e che viene ripreso anche dal successivo articolo 28, comma 3, lett. b).
La precedente categoria dei "dati sensibili" trova ora nuova collocazione nell'articolo 9 del Regolamento, rubricato "trattamento di categorie particolari di dati personali" il quale, al paragrafo 1, elenca la seguente serie di dati, riconducibili ai precedenti "dati sensibili":

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

Per un riferimento a quelli definiti in precedenza "dati giudiziari" si rinvia alla lettura dell'articolo 10 del Regolamento, rubricato "trattamento dei dati personali relativi a condanne penali e reati" mentre per i "dati anonimi" si veda l'articolo 11, che fa riferimento ai casi di "trattamento che non richiede l'identificazione".

L'articolo 5 del Regolamento 2016/679/UE sancisce quali sono i "**principi applicabili al trattamento di dati personali**". La scrupolosa osservanza di detti principi deve costituire il punto di riferimento dal quale il Titolare, i Responsabili e le Persone autorizzate al trattamento non devono per alcun motivo discostarsi nell'approcciare la tematica della protezione dei diritti delle persone in connessione al trattamento dei dati personali.

Tali principi si riportano, pertanto, di seguito:

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, 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, conformemente all'articolo 89, paragrafo 1, 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**»);
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. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («**responsabilizzazione**»).

In sintesi, i principi applicabili al trattamento di dati personali possono così riassumersi:

- **liceità, correttezza e trasparenza;**
- limitazione della finalità;
- minimizzazione dei dati;
- esattezza;
- limitazione della conservazione;
- integrità e riservatezza

e sono connessi strettamente al principio cardine della **responsabilizzazione,** in base al quale il Titolare del trattamento è responsabile per l'osservanza degli stessi e deve essere in grado, all'occorrenza, di dimostrarlo.

2. Condizioni di liceità del trattamento

L'articolo 6 del Regolamento specifica il primo dei principi applicabili al trattamento di dati personali, precisando che "*un 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;
[…]
e) il trattamento è **necessario per l'esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri **di cui è investito il titolare del trattamento**.

Al di fuori dei casi previsti, in particolare, dalle lettere c) ed e) del paragrafo 1 dell'articolo 6 del Regolamento, il trattamento dei dati da parte della Regione Campania è lecito pertanto **se sussiste il consenso dell'interessato per una o più specifiche finalità**.

A proposito del **consenso**, occorre tenere in debito conto quanto è riportato nei concetti introduttivi del Regolamento, detti "Considerando", in particolare del Considerando n. 42 ove si specifica che "*è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. […] Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in*

grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio".

Ancora a proposito del consenso, il Considerando n. 43 precisa che "*per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è* ***un'autorità pubblica*** *e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione".*

3. Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

Gli articoli 12 e seguenti del Regolamento 2016/679/UE sanciscono i diritti degli interessati in ordine al trattamento dei propri dati personali.
Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

Le informazioni previste dagli articoli 13 e 14 sono quelle che comunemente vengono raggruppate sotto il concetto di "Informativa" ed il nuovo Regolamento le disciplina distintamente a seconda se i dati personali siano raccolti **presso l'interessato** o **non siano stati raccolti presso l'interessato.**

Le comunicazioni previste dagli articoli da 15 a 22 e dall'articolo 34 sono invece quelle che attengono ai seguenti diritti:

a. Articolo 15 - Diritto di accesso dell'interessato;
b. Articolo 16 - Diritto di rettifica;
c. Articolo 17 - Diritto alla cancellazione ("diritto all'oblio");
d. Articolo 18 - Diritto di limitazione di trattamento;
e. Articolo 19 - Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;
f. Articolo 20 - Diritto alla portabilità dei dati (solo per le aziende commerciali);
g. Articolo 21 - Diritto di opposizione;
h. Articolo 22 - diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione;
i. Articolo 34 – Diritto a ricevere una comunicazione in caso di violazione dei dati personali.

Vediamo in sintesi il contenuto delle due Informative, per poi esaminare in seguito sinteticamente il contenuto dei diritti degli interessati sopra riportati:

3.1. Informazioni da fornire qualora i dati personali siano raccolti <u>presso</u> l'interessato

L'articolo 13 del Regolamento prevede un elenco di informazioni da fornire obbligatoriamente all'Interessato "nel momento in cui i dati personali sono ottenuti".
Le informazioni sono fornite per iscritto o con altri mezzi, anche con mezzi elettronici.

Tra le informazioni da fornire devono essere necessariamente incluse le seguenti, al fine di garantire il rispetto dei principi di correttezza e trasparenza:

a. L'indicazione del Titolare (Giunta Regionale della Campania) con l'indicazione della sede legale in Napoli, alla via Santa Lucia n. 81;
b. L'indicazione del dirigente Delegato al trattamento, con l'indicazione della sede dell'Ufficio che effettuerà il trattamento ed i dati di contatto (recapiti telefonici, e-mail, pec ecc.);
c. I dati di contatto del Responsabile della protezione dei dati;
d. Le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento (vedi precedente punto 2. "Condizioni di liceità del trattamento");
e. Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f. Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
g. 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;
h. Qualora il trattamento sia basato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
i. Il diritto di proporre reclamo a un'Autorità di controllo (in Italia, il Garante per la Privacy);
j. 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;
k. L'eventuale 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.

3.2. Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

Qualora i dati non siano stati raccolti presso l'interessato, l'articolo 14 del Regolamento prevede l'obbligo di fornire allo stesso, **oltre alle informazioni di cui al precedente punto 3.1.**, anche "le categorie di dati in questione" nonché "la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico".

Le informazioni che precedono devono essere fornite:
a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

L'articolo 14 prevede delle eccezioni all'obbligatorietà della comunicazione delle informazioni di cui in premessa, qualora e nella misura in cui ricorra una delle seguenti condizioni, che il Titolare deve essere in grado di provare e giustificare:

a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui

l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

3.3. Diritti degli Interessati al trattamento dei dati personali

Abbiamo riportato in precedenza sinteticamente i diritti degli Interessati che vedono trattare propri dati personali: passiamo ora ad una sintetica rassegna di tali diritti, rimandando alla lettura dei rispettivi articoli del Regolamento per la loro piena comprensione.

3.3.1. Diritto di accesso dell'interessato (articolo 15)

1. 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.

3.3.2. Diritto di rettifica (Articolo 16)

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

3.3.3. Diritto alla cancellazione ("diritto all'oblio") Articolo 17

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento 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 conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
[…]
3. I paragrafi 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 previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

3.3.4. Diritto di limitazione di trattamento (articolo 18)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento 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 il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, idati 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 ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

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

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

3.3.6. Diritto alla portabilità dei dati (Articolo 20);

Tale diritto è sostanzialmente esercitabile nei confronti di soggetti esercenti attività commerciali, pertanto non se ne forniscono ulteriori particolari. Si rinvia alla lettura dell'articolo 20 del Regolamento.

3.3.7. Diritto di opposizione (Articolo 21)

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) – **ossia quando il trattamento si sia reso 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 -, 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.

Sul punto, appare opportuno richiamare il contenuto del Considerando n. 69, che precisa:
"*Qualora i dati personali possano essere lecitamente trattati, essendo il trattamento necessario per l'esecuzione di un* ***compito svolto nel pubblico interesse*** *oppure* ***nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento****, ovvero per i legittimi interessi di un titolare del trattamento o di terzi, l'interessato dovrebbe comunque avere il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. È opportuno che* ***incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato***".

3.3.8. diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione (Articolo 22)

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 paragrafo 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 un titolare del trattamento;
b) 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 e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.

3.3.9. Diritto a ricevere una comunicazione in caso di violazione dei dati personali (Articolo 34)

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 paragrafo 1 del presente articolo 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 33, paragrafo 3, lettere b), c) e d).

PARTE SECONDA
Assetto privacy e misure organizzative

4. Organigramma privacy

Il Regolamento 2016/679/UE richiede anche alle Pubbliche Amministrazioni di dotarsi di un nuovo assetto organizzativo per fronteggiare i numerosi compiti che la normativa prevede. La Regione Campania, pertanto, per quel che concerne le strutture afferenti alla Giunta regionale, si organizza come segue:

1) Titolare del trattamento

Il "Titolare del trattamento" dei dati personali effettuati dalle Strutture organizzative della Giunta Regionale della Campania, in continuità con quanto previsto in vigenza delle normative precedenti, è la Giunta Regionale;

2) Delegati al trattamento

La Giunta Regionale, con proprio provvedimento, ha introdotto nell'organigramma della privacy la figura del "Delegato al trattamento", che prende il posto della figura del "responsabile interno" previsto dalla previgente normativa.

Delegati al trattamento sono pertanto tutti i Dirigenti in servizio presso la Giunta regionale, sia a tempo determinato che a tempo indeterminato, di ruolo o incaricati di incarico dirigenziale ai sensi della vigente normativa, ognuno per la parte di competenza relativa al trattamento dei dati personali effettuato nello svolgimento dell'incarico ricevuto, secondo le previsioni del rispettivo contratto individuale di lavoro;

3) Referenti privacy

Ogni Ufficio di livello dirigenziale (nell'attuale assetto organizzativo Uffici di Diretta Collaborazione del Presidente, Direzioni Generali, Uffici Speciali, Strutture di missione, Autorità di Audit, Strutture di Staff dotate o meno di autonomia, Unità operative dirigenziali) dovrà nominare un proprio "Referente privacy", che dovrà coadiuvare il Dirigente nell'espletamento dei molteplici compiti afferenti la tematica del trattamento dei dati personali svolti dall'Ufficio.

4) Responsabili esterni del trattamento

I Responsabili esterni sono tutti quei soggetti che, essendo "esterni" all'Amministrazione regionale (quali ad esempio società, consulenti, collaboratori, altri enti ecc.) trattano dati personali per conto dell'Amministrazione regionale.

Come espressamente previsto dall'articolo 28 del Regolamento 2016/679/UE, la legittimazione al trattamento di dati personali di cui è titolare la Giunta Regionale della Campania da parte di detti soggetti deve avvenire a seguito di stipula di apposito contratto, con le previsioni dettate dal citato articolo 28 nonché gli obblighi di cui agli articoli 30 e 33 del medesimo Regolamento.

5) Sub-responsabili esterni del trattamento

I Responsabili esterni del trattamento possono, se previamente autorizzati per iscritto e con idonea formalizzazione, affidare alcuni trattamenti di dati personali a sub-responsabili esterni.

I Responsabili esterni rimangono tuttavia, in tale caso, responsabili in solido per eventuali trattamenti illeciti o non conformi al Regolamento effettuati dai sub-responsabili. Si veda l'art. 28 del Regolamento.

6) Persone autorizzate al trattamento

La figura dell'Incaricato, di cui alla previgente normativa, non è più prevista dal Regolamento 2016/679/UE. Essa, tuttavia, è sostituita dalla figura delle "persone autorizzate al trattamento" dei dati personali. Si tratta di tutti quei soggetti che, all'interno di una Struttura dirigenziale e per le materie di competenza, effettuano trattamenti di dati personali nell'espletamento dei propri compiti istituzionali. Il Regolamento prevede che tali trattamenti avvengano sotto l'autorità diretta del Titolare o del Responsabile, i quali garantiscono che gli stessi si siano impegnati alla riservatezza o posseggano un adeguato obbligo legale di riservatezza.

7) Responsabile della protezione dei dati personali

Si tratta di una figura di nuova istituzione, disciplinata dagli articoli 37 a 39 del Regolamento, a cui sono affidati compiti di consulenza e sorveglianza.

4.1. Gruppo di Lavoro Regolamento 2016/679/UE.

Ai soggetti indicati al precedente punto 4., nell'assetto organizzativo privacy della Giunta Regionale della Campania, si affianca per assumere un ruolo di primo piano il "*Gruppo di Lavoro Regolamento 2016/679/UE*".
Si tratta di un gruppo con compiti operativi, di supporto, gestione, analisi e soluzione dei problemi applicativi del Regolamento.
Il Gruppo di Lavoro è così composto:
- Dirigente del Gabinetto del Presidente – Ufficio V "*Università, Ricerca e Innovazione. Istruzione, formazione, lavoro e politiche giovanili. Politiche culturali e turismo e politiche sociali. Supporto Verifica Attuazione Programma di Governo. Amministrazione digitale*" o suo delegato;
- Direttore Generale per le Risorse Umane o altro Dirigente delegato;
- Direttore Generale per l'Università, la Ricerca e l'Innovazione o altro Dirigente delegato;
- Direttore dell'Ufficio Speciale Avvocatura Regionale o altro Dirigente delegato;
- Responsabile della prevenzione della corruzione e della trasparenza o suo delegato;
- Responsabile della Transizione digitale.

Il coordinamento delle attività del *Gruppo di Lavoro Regolamento 2016/679/UE* è affidato al Responsabile della protezione dei dati personali.
Il *Gruppo di Lavoro Regolamento 2016/679/UE* potrà essere integrato con Delegati e/o Referenti privacy e/o componenti di altre strutture regionali in riferimento alle necessità di protezione dei dati personali dalle stesse gestiti.

5. Attribuzioni e compiti del Delegato

Il Delegato al trattamento – come individuato al punto 2) del precedente paragrafo 4. – esercita tutte le incombenza in materia di protezione dei dati personali per le materie di competenza del proprio Ufficio, avvalendosi per questo della collaborazione del Referente privacy (dallo stesso individuato) nonché, per le attività pratiche legate al trattamento, delle Persone autorizzate al trattamento, adeguatamente responsabilizzate sul tema.
Il Delegato al trattamento, in particolare, deve:
a. Osservare i principi applicabili al trattamento dei dati e le condizioni di liceità del trattamento, garantire la qualità dei dati personali, le corrette modalità di raccolta, conservazione e trattamento dei dati, anche da parte del personale autorizzato al trattamento del proprio Ufficio dirigenziale. Si ricorda che i principi applicabili ai trattamenti sono quelli previsti dall'articolo 5 del Regolamento, e dettagliati al paragrafo 1. del predetto documento (**Osservanza dei principi applicabili ai trattamenti**);
b. Fornire le Informative agli interessati di cui ai paragrafi 3.1. e 3.2. del presente documento **(Informative)**;
c. Tenere traccia del percorso logico e delle motivazioni che hanno condotto ad effettuare le scelte in materia di protezione dei dati **(Documentazione delle scelte)**;
d. Implementare, per le attività di competenza dell'Ufficio dirigenziale ricoperto, il Registro delle attività di trattamento, secondo le direttive ricevute dall'Amministrazione al momento dell'avvio del Registro **(Implementazione del registro)**;
e. Effettuare la valutazione dei rischi per le attività di trattamento e, se necessario ai sensi del Regolamento, la "valutazione di impatto" secondo le modalità indicate nel successivo paragrafo 10, nel rispetto e secondo le indicazioni fornite al Gruppo di Lavoro, sentito il parere, se richiesto, del Responsabile per la protezione dei dati **(Valutazione dei rischi e Valutazione di impatto);**
f. Adottare le misure di sicurezza adeguate alla tipologia di dati personali trattati, secondo le indicazioni fornite nel prosieguo del presente documento **(Misure di sicurezza)**;

g. Collaborare col Responsabile per la protezione dei dati, consentendo al medesimo eventuali verifiche relativamente all'organizzazione della privacy della propria struttura **(Collaborazione col RpD)**;

h. Autorizzare per iscritto le persone interne alla propria struttura che trattino dati personali e verificare che gli stessi siano trattati esclusivamente per le esigenze strettamente indispensabili allo svolgimento delle attività loro assegnate.

Autorizzare, con le medesime modalità, anche eventuali collaboratori esterni all'Amministrazione persone fisiche operanti stabilmente all'interno della struttura, a prescindere dalla tipologia di rapporto contrattuale intrattenuto (es. stagisti, tirocinanti, co.co.co. ecc.) (**Autorizzazione al trattamento**);

i. Formalizzare, mediante apposito contratto, la nomina di eventuali "Responsabili esterni" al trattamento dei dati personali gestiti dalla propria struttura, in tutti i casi in cui ad un soggetto "esterno" all'Amministrazione regionale (persona fisica o giuridica, pubblica o privata) siano affidate attività di trattamento che presuppongono l'esercizio di un potere decisionale autonomo (ad es. società di consulenza, società di gestione di applicativi informatici attraverso i quali vengono gestiti dati personali, avvocati esterni all'Amministrazione ecc.). Si rinvia per gli opportuni approfondimenti alla lettura degli articoli 28, 30 e 33 del Regolamento. Se al soggetto esterno è affidata l'amministrazione di sistemi informativi, lo stesso deve essere investito dal Delegato anche del compito di "Amministratore di sistema", ai sensi del provvedimento del Garante per la privacy del 27.11.2008 sugli amministratori di sistema (**Nomina di Responsabili "esterni"**)

j. Nei casi di eventuali violazioni dei dati personali (c.d. data breach), anche avvenute presso responsabili esterni o loro sub-responsabili, adottare tutte le misure riportate nei paragrafi seguenti, compresa l'implementazione dell'apposito registro dei data breach (**Databreach**);

k. Individuare all'interno della struttura diretta un Referente Privacy, con il compito di coadiuvarlo nella gestione delle problematiche connesse al trattamento ed alla protezione dei dati personali gestiti dalla struttura nonché nell'adempimento puntuale di tutti gli obblighi previsti dalla normativa vigente. Il Referente Privacy si interfaccerà, qualora necessario, con il Gruppo di Lavoro Regolamento 2016/679/UE nonché con il Responsabile per la protezione dei dati, cui il relativo nominativo – così come le eventuali sostituzioni – andranno tempestivamente comunicati.

6. Registro delle attività di trattamento

Una delle innovazioni previste dal Regolamento è l'introduzione, prevista dall'articolo 30, dell'obbligo della tenuta di un "Registro delle attività di trattamento".

Il Registro è unico per tutta l'Amministrazione della Giunta Regionale e – a richiesta – deve essere messo a disposizione del Garante per la privacy o altre autorità di controllo, ai fini della verifica della correttezza nella gestione e trattamento dei dati personali.

Il Registro ha una funzione descrittiva e dovrà essere implementato tempestivamente da ogni Struttura dirigenziale.

Detto Registro, che sarà tenuto nelle forme e con le modalità stabilite dal Gruppo di Lavoro, deve contenere almeno le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

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, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

7. Violazione dei dati personali. Nozione e adempimenti connessi. Tenuta del Registro dei databreach

L'articolo 33 del Regolamento prescrive inoltre l'obbligo di tenere un "Registro dei databreach"; recita infatti l'articolo 33 che "il titolare del trattamento [e per esso il suo delegato n.d.r.] documenta qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze ed i provvedimenti adottati per porvi rimedio.
In tale registro devono essere annotate anche le violazioni dei dati personali avvenute presso i responsabili esterni del trattamento o eventuali loro sub-responsabili, per quanto attiene il trattamento dei dati ad essi affidati.
Anche il Registro dei databreach viene tenuto nelle forme e con le modalità previste dal Gruppo di Lavoro.

Il Regolamento, oltre alla tenuta dell'apposito Registro, prevede una serie di attività da porre in essere qualora si dovessero verificare violazioni di dati personali.

L'articolo 33 del Regolamento prescrive infatti che "*per le violazioni di dati personali, che comportino 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 […] il Titolare del trattamento [e per esso il suo Delegato n.d.r.] notifica la violazione all'autorità di controllo competente (Garante per la Privacy) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto 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. Qualora la notifica all'autorità di controllo non sia effettuata entro le 72 ore, è corredata dei motivi del ritardo.*

Si richiama l'attenzione di ciascun Delegato al puntuale rispetto dell'obbligo appena descritto, così come la necessità di impartire le opportune disposizioni a tutte le "persone autorizzate al trattamento" presso la propria struttura affinché trattino correttamente i dati personali da essi gestiti ed informino con la massima tempestività il Delegato di eventuali violazioni rilevate, affinché questo possa essere posto in condizioni di ottemperare alla citata segnalazione.

In caso di violazione di dati personali, l'articolo 34 del Regolamento prevede, a determinate condizioni, l'obbligo di avvisare l'interessato circa l'avvenuta violazione. Prevede infatti il Regolamento che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è obbligatorio comunicare la violazione all'interessato senza ingiustificato ritardo.
Ci sono tuttavia delle eccezioni a tale obbligo, riportate al paragrafo 3 dell'articolo 34:

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 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 paragrafo 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 analoga efficacia.

Il Delegato, pertanto, in caso di violazione di dati personali, è tenuto ad effettuare, con la collaborazione del proprio Referente Privacy, apposita documentata istruttoria, dalla quale emergano le scelte effettuate in ordine alla necessità o meno di comunicare la violazione al destinatario, sulla base degli elementi riportati nell'articolo 34 del Regolamento.

PARTE TERZA
Sicurezza dei dati, rischi, misure tecniche

8. Nozione di sicurezza

Fondamentale ai fini del perseguimento degli obiettivi connessi alla protezione dei dati personali è la conoscenza e la consapevolezza, da parte dei Delegati e delle persone da esse autorizzate al trattamento, della natura e della delicatezza dei dati personali trattati. Solo in tal modo è possibile procedere all'analisi dei rischi connessi al trattamento ed alla conseguente adozione delle misure di protezione da adottare. Proprio di questo processo logico va fornita evidenza nel Registro delle attività di trattamento, descritto al precedente paragrafo 6.

Il Considerando n. 39 del Regolamento specifica che "i dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento".

I dati personali, com'è evidente, possono essere trattati e conservati in formato digitale o su supporto cartaceo, motivo per il quale le misure di sicurezza da adottare devono essere differenti ed adeguate alle diverse situazioni e natura dei dati da trattare. Nel prosieguo del presente documento si riportano alcune misure tecniche minime da adottare per la protezione delle due tipologie di dati.

In ogni caso, ciascun Delegato ha il'obbligo di adottare ogni ulteriore e più adeguata misura di sicurezza, che sia ritenuta necessaria, all'esito dell'analisi dei rischi di cui si darà conto nel successivo paragrafo 9, in relazione alla particolare tipologia ed al metodo dei trattamenti effettuati presso la propria Struttura, tenendo conto in particolare dei rischi derivanti dalla possibile distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati.

L'articolo 32 del Regolamento precisa infatti che è necessario *[…]*
mettere in atto misure tecniche 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 cifratura dei dati personali;
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.

9. Analisi dei rischi

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:
- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Questo è il concetto di **rischio** precisato dal Considerando n. 75 del Regolamento.

Il successivo Considerando n. 76 precisa che "*la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*".

Discende dai concetti sopra descritti l'importanza di procedere all'individuazione del rischio connesso al trattamento, alla sua **valutazione** in termini di origine, natura, probabilità e gravità nonché all'individuazione delle migliori prassi per attenuare il rischio.

10. Valutazione d'impatto sulla protezione dei dati (Privacy Impact Assessment) – P.I.A.

Il Regolamento 2016/679/UE introduce un adempimento innovativo nel campo della protezione dei dati personali: la Valutazione d'impatto (P.I.A.), di cui fornisce definizione e contenuti negli articoli 35 e seguenti.
Nell'ambito degli Uffici della Giunta Regionale della Campania, tale valutazione sarà effettuata dai Delegati nel rispetto e in attuazione degli indirizzi tecnico-operativi formulati dal Gruppo di Lavoro, che potrà avvalersi, in ciò, della consulenza del Responsabile per la protezione dei dati personali.

Le motivazioni per le quali è importante procedere alla valutazione d'impatto sono richiamate nel Considerando n. 84 al Regolamento, che recita:

"*Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un* ***rischio elevato*** *per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento.*
Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo".

L'articolo 35 del Regolamento precisa:

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La Valutazione d'impatto – P.I.A. – è inoltre richiesta ogniqualvolta "l'*uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

Il paragrafo 4 dell'articolo 35 prevede che l'autorità di controllo (Garante per la Privacy) redigerà un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione.

Il Gruppo di Lavoro, in ogni caso, nel predisporre i propri indirizzi tecnico-operativi finalizzati all'eventuale Valutazione d'impatto, nelle more dell'adozione del citato elenco da parte del Garante, si atterrà a quanto previsto nelle **Linee Guida WP 248** adottate in data 04.04.2017 e revisionate in data 04.10.2017 dal GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI istituito in virtù dell'articolo 29 della direttiva 95/46/CE.

11. Misure tecniche per la protezione dei dati personali

Secondo quanto previsto dall'art. 32 del Regolamento il Titolare e il responsabile del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio, devono adottare le **misure tecniche e organizzative adeguate** per garantire un **livello di sicurezza adeguato al rischio**.

Nell'art. 32 del Regolamento è detto che le misure di sicurezza comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
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.

Si tratta di un'elencazione aperta e non esaustiva (si legge nella norma "tra le altre, se del caso"), tenuto conto che il Titolare/Delegato è chiamato a valutare e adottare, caso per caso, le misure che dovesse ritenere necessarie alla massima protezione dei dati personali gestiti dalla propria struttura.

Ci si pone la domanda sul se le misure minime previste dagli articoli 33 e seguenti del Codice privacy (D. Lgs. 196/2003) possano/debbano trovare ancora applicazione.

Al quesito risponde lo stesso Garante per la Privacy, il quale, nella propria Guida al Regolamento in materia di protezione dei dati personali – alla cui lettura si invitano tutti i Delegati nonché le persone autorizzate al trattamento della Giunta Regionale della Campania - "*non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza".*
Tuttavia – rileva il Garante – *"l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni*".
In concreto allora, le misure minime di sicurezza non potranno continuare a essere considerate misure obbligatorie, **ma è possibile ritenere che esse rappresentino il nucleo centrale minimo per garantire la sicurezza dei dati.**

Per tale motivo, si riportano di seguito, con le precisazioni e nei limiti appena segnalati, le misure (tecniche) minime di sicurezza previste dall'Allegato B. del D. Lgs. 196/2003, che distingue a seconda che il trattamento dei dati avvenga con strumenti elettronici ovvero senza l'ausilio di detti strumenti:

A) TRATTAMENTI CON STRUMENTI ELETTRONICI

Modalità tecniche da adottare in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una

parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies*del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

B) TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.