ISTRUZIONI
per i trattamenti
di dati personali

Misure organizzative e tecniche

Regione del Veneto

GIUNTA REGIONALE

PARTE PRIMA
INQUADRAMENTO GENERALE E MISURE ORGANIZZATIVE

Premessa

Il Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016, noto anche come *General Data Protection Regulation* (**GDPR**), 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 1995/46/CE*, si applica - senza necessità di essere recepito - in tutti gli Stati membri dell'Unione Europea a partire dal **25 maggio 2018**.
Per effetto di tale nuova normativa europea la protezione dei dati personali subisce un profondo rinnovamento.
La principale novità introdotta dal predetto Regolamento Europeo è il principio della "***responsabilizzazione***" ("*accountability*") che attribuisce al Titolare e, più in generale, a chi tratta dati personali 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, perciò, intende fornire direttive e istruzioni per i trattamenti di dati personali effettuati dall'Amministrazione regionale, fermo restando che il citato GDPR deve essere comunque rispettato in tutte le sue parti, anche quelle non richiamate di seguito, e che la disciplina rilevante in materia di protezione dei dati personali si compone anche delle indicazioni e delle linee guida che saranno fornite dal Garante Privacy nonché, eventualmente, dal Legislatore italiano che potrebbe integrare la disciplina con ulteriori norme nazionali.

1. Definizioni

Le definizioni più rilevanti di cui all'articolo 4 del GDPR sono le seguenti:

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;

[...]

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;
[…]
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 […]

Tra le definizioni sopra elencate non compaiono più, rispetto al D.Lgs. 196/2003 (Codice Privacy), le definizioni di: Incaricato, dati sensibili, dati giudiziari e dati anonimi.
A proposito degli Incaricati, tuttavia, al punto n. 10, nella definizione di "*terzo*" compare un accenno alle "*persone autorizzate al trattamento*", assimilabile alla "vecchia" figura dell'Incaricato.
Per quanto riguarda i "*dati sensibili*", l'articolo 9, rubricato <<***trattamento di categorie particolari di dati personali***>>, al paragrafo 1, elenca i seguenti dati, riconducibili ai "vecchi" 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.

Con riferimento ai "*dati giudiziari*", l'articolo 10, è rubricato semplicemente ***<<trattamento dei dati personali relativi a condanne penali e reati>>***.
Per i "*dati anonimi*", invece, l'articolo 11 fa riferimento, semplicemente, ai casi di << ***trattamento che non richiede l'identificazione***>>.

2. Principi applicabili al trattamento dei dati

L'articolo 5 del GDPR, rubricato "***Principi applicabili al trattamento di dati personali***", elenca i princìpi ispiratori della disciplina riguardante la protezione dei 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; […]
(«***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 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***»).

Un corollario importante che discende dal principio di "*responsabilizzazione*" e che si collega ai sopra elencati princìpi, è quello per cui è necessario che sia **documentato ogni adempimento**.
La **documentazione delle scelte** – a fascicolo – risulta indispensabile, inoltre, per ricostruire *a posteriori* ai motivi delle scelte effettuate e poter così dimostrare (laddove eventualmente richiesto) la bontà e la correttezza delle scelte effettuate, nonché delle azioni intraprese.

All'articolo 25 vengono poi codificati i princìpi della <<***privacy by design***>> e della <<***privacy by default***>>. Il primo dei due principi impone (sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso) di mettere <<*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.*>>
Il secondo principio impone che <<*siano trattati, per impostazione predefinita* ["**by default**"], *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.*>>

3. Condizioni di liceità del trattamento

Ai sensi dell'articolo 6 del GDPR un <<*trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni*>> (si riportano quelle rilevanti per una Pubblica Amministrazione):

> [...]
> 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;

Il "**Considerando n. 45**", introduttivo al Regolamento europeo, precisa che il GDPR << ***non*** *impone che vi sia un atto legislativo specifico per ogni singolo trattamento.* ***Un atto legislativo*** *può essere sufficiente come base per* ***più trattamenti*** *effettuati conformemente a un obbligo legale cui è soggetto il titolare del trattamento* ***o*** *se il trattamento è necessario per l'esecuzione di un* ***compito svolto*** *nel pubblico interesse o per l'esercizio di pubblici poteri.*>>

Al di fuori delle ipotesi sopra descritte, il trattamento è lecito, ai sensi del medesimo articolo, se:

> a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

Tuttavia, a proposito della possibilità per una Pubblica Amministrazione di richiedere tale consenso il "**Considerando n. 42**" chiarisce 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.*>>

Per i trattamenti connessi alle "***categorie particolari di dati personali***" il trattamento – invece – è consentito solo in presenza di determinate condizioni, ossia se è: "*necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, 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*" (art. 9, par. 2, lett. g).
Relativamente a questa categoria di dati, si evidenzia che il divieto di trattare tali dati viene meno se <<*il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato*>> (art. 9, par. 2, lett. e).

4. I diritti degli Interessati

Si riportano, di seguito, i più rilevanti diritti degli Interessati.

L'Interessato ha diritto di ricevere le informazioni relative al trattamento 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 (Art. 12, par. 1). Sul punto si rinvia - più oltre - per i contenuti al punto relativo all'<<INFORMATIVA>>.

L'interessato ha diritto di ricevere riscontro alla sua richiesta 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'interessato deve essere informato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta (art. 12, par. 3).

Nel caso in cui non sia possibile ottemperare alla richiesta dell'Interessato, l'Interessato ha diritto di riceverne notizia senza ritardo, e al più tardi entro un mese dal ricevimento della sua richiesta, dei motivi dell'inottemperanza nonchè della possibilità di proporre reclamo a un'Autorità di Controllo e di proporre ricorso giurisdizionale (art. 12, par. 3).

Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato, purché sia comprovata l'identità dell'interessato (art. 12, par. 3).

L'Interessato ha il diritto di ottenere 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 che lo riguardano, senza lesioni per i diritti e le libertà altrui (art. 15).

L'interessato ha il diritto di ottenere 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 (art. 16).

Per quanto riguarda il "Diritto alla cancellazione" («***diritto all'oblio***») si riporta di seguito un estratto dell'art. 17.

> 1. L'interessato ha il diritto di ottenere [...] la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo [...], 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;
> [...]
> d) i dati personali sono stati trattati illecitamente;
> e) i dati personali devono essere cancellati per adempiere un obbligo legale
> [...]
>
> 2. Il Titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari 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 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 [...] 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;
c) per motivi di interesse pubblico nel settore della sanità pubblica [...];
d) 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 paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Secondo quanto precisato nel **Considerando n. 66**, inoltre:

Per rafforzare il «*diritto all'oblio*» nell'ambiente *online*, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi *link* verso tali dati personali o copia o riproduzione di detti dati personali.

L'Interessato ha diritto che eventuali rettifiche o cancellazioni o limitazioni del trattamento dei dati che lo riguardano siano portate a conoscenza di ciascuno dei destinatari a cui i dati personali sono stati comunicati, <<*salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato*>> (art. 19). L'Interessato ha diritto di sapere quali sono i destinatari a cui i dati sono stati trasmessi, "*qualora l'Interessato* [medesimo] *lo richieda*".

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, lett. e) 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*" (cfr. art. 21). "*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*" (art. 21, par. 1). Su questo punto – ad integrazione di quanto sopra – è opportuno prendere visione anche del **Considerando n. 69**:

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.

5. Informativa

A) Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

L'articolo 13 del GDPR 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, se del caso, con mezzi elettronici.
Tra queste informazioni si devono includere le seguenti, necessarie per garantire un trattamento corretto e trasparente:

- Il Titolare (Regione del Veneto/Giunta Regionale) con l'indirizzo della sede;
- Il Delegato al trattamento con l'indirizzo della sede e i dati di contatto;

- Il *Data Protection Officer* (Responsabile della protezione dei dati) con l'indirizzo della sede e i dati di contatto;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento (cfr. "3. Condizioni di liceità del trattamento");
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- 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;
- il diritto di proporre reclamo a un'autorità di controllo (Garante Privacy);
- 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;
- l'esistenza (eventuale) di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'art. 13, par. 3, prescrive che <<*Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una* ***finalità diversa*** *da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente [...]*>>.

Unica eccezione per evitare di fornire le informazioni sopra descritte è ammessa <<*se e nella misura in cui l'interessato dispone già delle informazioni*>>, ma occorre essere in grado di dimostrarlo, nel rispetto del principio della documentazione delle scelte.

B) Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

Ai sensi dell'art. 14 <<*qualora i dati non siano stati ottenuti presso l'interessato*>> è obbligatorio fornire all'interessato le informazioni di cui alla precedente lett. A), integrate con "*le categorie di dati in questione*" (cfr. art. 14, par. 1, lett. d) 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*>> (cfr. art. 14, par. 1, lett. f).

Le informazioni devono essere fornite all'Interessato:

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.

Per quanto riguarda le eccezioni, si riportano di seguito quelle elencate all'art. 14, par. 5, da applicarsi <<*se e nella misura in cui*>>:

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, [...], o nella misura in cui l'obbligo [...] 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;

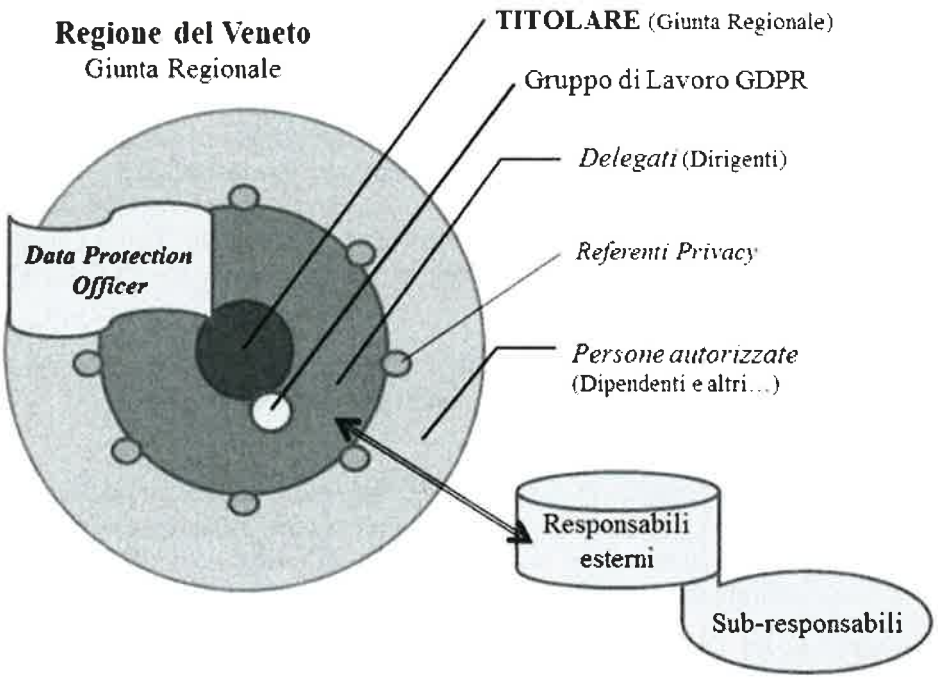
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure

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.

Anche nel caso di queste eccezioni occorre essere in grado di dimostrare la sussistenza delle condizioni per l'applicazione delle eccezioni medesime, nel rispetto del principio della documentazione delle scelte.

6. L'assetto organizzativo privacy

Il GDPR impone di dotarsi di un nuovo "*assetto organizzativo privacy*", e quello dell'Amministrazione regionale, per quanto attiene alle strutture afferenti alla Giunta regionale, è raffigurabile come segue:



I componenti di questo nuovo assetto sono, dunque, i seguenti:

a) Titolare del trattamento

Il "*Titolare del trattamento*" di dati personali, effettuati dalle strutture regionali della Giunta Regionale, in linea con quanto fino ad ora sempre disposto fin dalla prima applicazione della normativa sulla privacy (risalente al 1997), rimane la Giunta Regionale.

b) Gruppo di lavoro GDPR

Gruppo di lavoro con compiti operativi, di gestione, supporto, analisi e soluzione dei problemi applicativi del GDPR, costituito nella seguente composizione:

- Segreteria della Giunta Regionale;
- Segreteria Generale della Programmazione;
- Area Programmazione e Sviluppo Strategico;

- Area Capitale Umano, Cultura e Programmazione Comunitaria;
- Area Sanità e Sociale – Direzione Risorse Strumentali SSR;
- Direzione Relazioni Internazionali, Comunicazione e SISTAR – Unità Organizzativa Comunicazione e Informazione;
- Direzione ICT e Agenda digitale;
- Direzione Organizzazione e Personale;
- Avvocatura;

L'individuazione dei componenti per ciascuna struttura sopra indicata e il coordinamento delle attività del Gruppo di lavoro, compresa la conservazione della relativa documentazione, è demandata al Direttore dell'Area Programmazione e Sviluppo Strategico.
Il Data Protection Officer, unitamente a funzionari della propria struttura, partecipa agli incontri del Gruppo di lavoro per esercitare le funzioni di cui all'art. 39 del GDPR.
Il "Gruppo di Lavoro GDPR" potrà essere integrato con Delegati e/o Referenti privacy e/o componenti di altre strutture regionali che possano essere interessate alla normativa in oggetto e coinvolte, di volta in volta, nelle problematiche in questione.

c) Delegati al trattamento
Viene introdotta nell'Amministrazione regionale la figura "intermedia" del "*Delegato al trattamento*" che subentra alla "vecchia" figura del Responsabile "interno", non più prevista.
Tenuto conto della complessità e della molteplicità delle funzioni istituzionali dell'Amministrazione Regionale, in cui le scelte di gestione finanziaria, tecnica e amministrativa (compresa la possibilità di stipulare contratti) rientrano tra le specifiche competenze dei Dirigenti (chiamati a dare attuazione alla programmazione dell'organo politico ed a realizzare gli obiettivi prefissati) nonché del loro ruolo centrale nel trattamento dei dati personali – fermo restando quanto disposto in tema di assetto organizzativo dell'Amministrazione Regionale – sono delegati tutti i Dirigenti in servizio presso l'Amministrazione Regionale, ognuno per la parte di propria competenza, al trattamento di dati personali effettuato nello svolgimento dell'incarico ricevuto, secondo quanto previsto dal rispettivo contratto individuale di lavoro.

d) Referenti privacy
I Referenti privacy sono i soggetti che, presso la struttura regionale di appartenenza, coadiuvano il Direttore nonché le persone autorizzate al trattamento nel disbrigo degli "adempimenti privacy".

e) Responsabili "esterni" del trattamento
I Responsabili "esterni" sono i soggetti che, essendo appunto "esterni" all'Amministrazione regionale (ad es. società, consulenti, enti, ecc.), trattano dati personali per conto dell'Amministrazione regionale sulla base di un contratto che deve prevedere anche quanto indicato all'articolo 28 del GDPR, in particolare al paragrafo 3, nonché gli obblighi di cui agli artt. 30 e 33, par. 2, del GDPR.

f) Sub-responsabili (esterni) del trattamento
I Responsabili "esterni" di cui alla lettera precedente (se previamente autorizzati per iscritto) possono affidare (eventualmente, con idonea formalizzazione) alcuni trattamenti di dati personali a "sub-responsabili esterni". Tale evenienza, tuttavia, non li esime dal rispondere in solido per ogni eventuale trattamento illecito o non conforme al GDPR effettuato dai sub-responsabili (art. 28, paragrafi 2 e 4).

g) Persone autorizzate al trattamento
La figura dell'Incaricato non è più prevista dal GDPR. Al suo posto viene introdotta, però, la figura delle "*persone autorizzate al trattamento*" di dati personali.

h) Data Protection Officer.
Il Responsabile della Protezione dei dati personali, meglio noto come "*Data Protection Officer*" (DPO) è una figura nuova, trasversale all'organizzazione, con compiti di consulenza e sorveglianza (artt. da 37 a 39).

7. Compiti dei Delegati

Il Delegato, come definito nel punto "6. L'assetto organizzativo privacy", nell'ambito delle proprie funzioni, al fine di poter fare efficacemente fronte alle diverse incombenze proprie del ruolo e di seguito indicate, si avvale della fattiva collaborazione dei Referenti privacy e delle persone autorizzate al trattamento, adeguatamente responsabilizzati sul tema.

Il Delegato, in particolare, con il predetto supporto, 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 degli stessi, anche da parte del *personale autorizzato* della propria struttura, secondo quanto disposto dal GDPR e vigilare sul rispetto delle istruzioni impartite. (**VERIFICA DEI TRATTAMENTI DI DATI**);

b) tenere traccia del percorso logico e delle motivazioni che hanno condotto ad effettuare le scelte in ambito privacy (**DOCUMENTAZIONE DELLE SCELTE**);

c) fornire le Informative agli Interessati (**INFORMATIVE**);

d) implementare per la struttura il Registro (unico) delle attività di trattamento, secondo le istruzioni ricevute al momento dell'avvio del Registro dell'Amministrazione regionale (**IMPLEMENTAZIONE DEL REGISTRO**);

e) effettuare la valutazione dei rischi per le attività di trattamento e, se necessario, la valutazione di Impatto (*Privacy Impact Assessment* – P.I.A.) nei casi e secondo le modalità specificate nel proseguo (**RISCHI E P.I.A.**) nonché nel rispetto e in attuazione degli indirizzi tecnico-operativi espressi dal Gruppo di Lavoro GDPR al fine di supportare ed agevolare i Delegati nell'adempimento dei propri compiti, con il parere, se richiesto, del *Data Protection Officer* (art. 39, par. 1, lett. c);

f) preoccuparsi dell'adozione delle misure di sicurezza adeguate, per quanto di competenza, come indicato nel proseguo (**MISURE DI SICUREZZA**);

g) coinvolgere tempestivamente e adeguatamente, in tutte le questioni riguardanti la protezione dei dati personali, il Data Protection Officer e collaborare con il medesimo per ogni questione relativa al trattamento dei dati, consentendo altresì verifiche privacy presso la propria struttura (**RAPPORTI COL DATA PROTECTION OFFICER**);

h) autorizzare al trattamento per iscritto le persone della propria struttura che trattano dati personali e verificare che questi trattino i dati personali strettamente indispensabili per lo svolgimento delle attività loro assegnate. Autorizzare al trattamento, altresì, anche eventuali collaboratori "esterni" (persone fisiche) all'Amministrazione, a prescindere dal rapporto contrattuale intrattenuto con l'Amministrazione (ad es. stagisti, tirocinanti, ecc.), purché non dotati di potere decisionale autonomo e stabilmente presenti negli uffici dell'Amministrazione. (**AUTORIZZAZIONI AL TRATTAMENTO**);

i) in tutti i casi in cui ad un soggetto "esterno" all'Amministrazione regionale (persona fisica o giuridica, pubblica o privata), siano affidate operazioni di trattamento che presuppongono l'esercizio di un potere decisionale autonomo accanto a quello di livello superiore del Delegato (ad es. avvocati "esterni", società di consulenza, ecc.), quest'ultimo deve provvedere a formalizzare - mediante contratto - la nomina di Responsabile "esterno" del trattamento secondo quanto indicato nell'art. 28 del GDPR, prevedendo o meno la possibilità per il Responsabile esterno di ricorrere a sub-responsabili e richiamando esplicitamente gli obblighi di cui agli artt. 30 e 33, par. 2, del GDPR (**NOMINA RESPONSABILE "ESTERNO"**).
Se al soggetto esterno è affidata l'amministrazione di sistemi informatici, esso deve essere investito dal Delegato anche del compito di "Amministrazione dei Sistemi", ai sensi del Provvedimento del Garante del 27.11.2008 sugli Amministratori di Sistema.

j) nei casi di violazioni di dati personali (*databreach*), avvenuti anche presso i responsabili "esterni" o loro eventuali sub-responsabili (per quanto attinente ai trattamenti di dati affidati), adottare le misure indicate nel proseguo (cfr. Violazione di dati – *databreach*), compresa l'implementazione del Registro dei databreach (**DATABREACH**);

k) individuare all'interno della propria struttura (di regola a livello di Area e Direzione) un "*Referente Privacy*" che si interfaccia con il Gruppo di Lavoro GDPR e con il *Data Protection Officer* per l'analisi delle questioni che interessano la struttura di appartenenza. Il nominativo ed ogni successiva sostituzione del Referente devono essere tempestivamente comunicati al *Data Protection Officer* (**COMUNICAZIONE REFERENTE PRIVACY**), indicando nella comunicazione:

codice struttura	nome struttura	cognome e nome del *Referente Privacy*	telefono

8. Compiti del Data Protection Officer

Il *Data Protection Officer*, nell'ambito delle proprie funzioni (artt. da 37 a 39), deve essere <<*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*>> ed <<*è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti*>> (art. 38).
Egli è - inoltre - dotato delle <<*risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*>>, compresa una sede consona al ruolo e funzionale - per prossimità - alle funzioni di consulenza e sorveglianza che deve svolgere.

Gli interessati possono contattare il *Data Protection Officer* per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.

Secondo quanto previsto dall'art. 39, in particolare, il *Data Protection Officer* deve:

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 ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il Data Protection Officer deve avere accesso diretto – in consultazione – al **Registro delle attività di trattamento**, ai fini della sorveglianza sull'osservanza degli obblighi e "adempimenti privacy", nonché al **Registro dei databreach** (articolo 33, par. 5).

Il Data Protection Officer può svolgere verifiche (AUDIT), a campione, per verificare il rispetto degli "adempimenti privacy".

9. Il Registro delle attività di trattamento e il Registro dei databreach

L'articolo 30 del GDPR introduce l'obbligo di tenere un "*Registro delle attività di trattamento*", unico per tutta l'Amministrazione regionale, che - a richiesta - può essere messo a disposizione dell'Autorità di controllo (Garante Privacy – Guardia di Finanza, *Nucleo Speciale Privacy*).

Il Registro ha una funzione descrittiva e deve essere aggiornato da ogni struttura regionale.
Costituisce il fondamento per altri adempimenti nonché il "*cruscotto informativo*" per la sorveglianza sul rispetto del GDPR.
Deve essere inteso, altresì, come un "*gestionale*" che consente di monitorare costantemente la situazione.

Tale Registro contiene tutte 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 [...];
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 [...].

Il Registro delle attività di trattamento si pone anche come strumento correlato all'analisi dei rischi che il Delegato è tenuto ad effettuare per i trattamenti di dati di propria competenza (cfr. oltre).

Il *Registro delle attività di trattamento* viene tenuto nelle forme e con le modalità stabilite dal "Gruppo di lavoro GDPR".

E' necessario tenere, inoltre, un "*Registro dei databreach*" come prescrive l'articolo 33, par. 5, *<<il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.>>*

In tale "*Registro dei databreach*" devono essere registrati anche i databreach avvenuti presso i responsabili "esterni" o loro eventuali sub-responsabili (per quanto attinente ai trattamenti di dati affidati).

Il *Registro dei databreach* viene tenuto nelle forme e con le modalità stabilite dal "Gruppo di lavoro GDPR".

Il Data Protection Officer deve avere accesso diretto – in consultazione – ai suddetti *Registro delle attività di trattamento* e *Registro dei databreach*.

PARTE SECONDA
LA SICUREZZA DEI DATI E MISURE TECNICHE

1. Introduzione sulla sicurezza

I dati personali, siano essi in formato digitale oppure su supporto cartaceo, devono essere custoditi con cura al fine di preservarne le caratteristiche di integrità, disponibilità e confidenzialità.

Il **Considerando n. 39** 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*".

Il principio della "***responsabilizzazione***" ("*accountability*") impone 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*".
Tra queste misure ve ne sono alcune di rilevanti <<*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.*>>

In ragione del fatto che i trattamenti possono essere effettuati con o senza l'ausilio di strumenti elettronici, le misure di sicurezza da adottare devono essere differenti ed adeguate alle diverse situazioni ed alla natura dei dati trattati.

Rientra, in ogni caso, tra i compiti del Delegato l'adozione di ulteriori e più adeguate misure di sicurezza, ritenute necessarie per la particolare tipologia dei dati trattati presso la propria struttura.

L'articolo 32 del GDPR precisa che è necessario mettere…

> …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 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.

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 (cfr. più oltre l'analisi dei rischi).

2. Censimento del patrimonio informativo

Ogni Delegato ed ogni persona autorizzata al trattamento devono conoscere ed essere consapevoli della natura e della delicatezza dei dati personali trattati.
La conoscenza di questi elementi è propedeutica a qualsiasi valutazione dei rischi sui dati trattati ed alla conseguente individuazione delle contromisure da adottare.
Il *Registro delle attività di trattamento* (più sopra descritto) ha la funzione, tra le altre, di raccogliere e dare evidenza degli elementi sinora indicati.

3. Analisi dei rischi

Il GDPR introduce il problema dei rischi nel **Considerando n. 75** che si riporta di seguito:

> 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.

Il successivo **Considerando n. 76** aggiunge:

> 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.

Da quanto sopra indicato risulta chiara l'importanza dell'*<<individuazione del rischio connesso al trattamento, la sua **valutazione** in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio.>>*

La valutazione del rischio è collegata all'attività di implementazione del Registro delle attività di trattamento. A sua volta tale valutazione – se rischi sono elevati – può condurre ad effettuare anche una valutazione d'impatto (*Privacy Impact Assessment* - P.I.A.). Si deve tener conto del fatto che i rischi possono variare nel corso del tempo, per cui la gestone del rischio è un "processo continuo".

4. Privacy Impact Assessment (P.I.A.)

La valutazione d'impatto (PIA) è disciplinata all'articolo 35 del GDPR e per essa, nel rispetto e in attuazione degli indirizzi tecnico-operativi espressi dal Gruppo di Lavoro GDPR al fine di supportare ed agevolare i

Delegati nell'adempimento dei propri compiti, può essere richiesta la collaborazione, sotto forma di parere, del *Data Protection Officer* (articolo 39, par. 1, lett. c).

Il **Considerando n. 84** inquadra il motivo per cui è importante la valutazione d'impatto:

> 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.

Il paragrafo 3 dell'articolo 35 precisa:

> La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 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 PIA è, altresì, richiesta nei casi che saranno indicati dal Garante Privacy in un apposito elenco e, comunque, 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*>>.

5. Violazioni di dati personali ("databreach")

Per le violazioni di dati personali (che comportano <<*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 GDPR stabilisce, all'articolo 33, paragrafo 1, che:

> In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente [...] 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 72 ore, è corredata dei motivi del ritardo.

Si intendono oggetto dell'eventuale obbligo di notifica, di cui sopra, anche i "*databreach*" avvenuti presso i responsabili "esterni" o loro eventuali sub-responsabili (per quanto attinente ai trattamenti di dati affidati).

Per ottemperare agli obblighi suddetti ogni Delegato, non appena venuto a conoscenza di un *databreach*, effettuata una prima necessaria istruttoria e valutati i rischi per i diritti e le libertà delle persone fisiche, avvisa tempestivamente la Direzione ICT e Agenda Digitale e il Data Protection Officer, perché quest'ultimo deve essere <<*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*>>.

Il Direttore della Direzione ICT e Agenda Digitale, sulla base degli esiti della predetta istruttoria del Delegato, viene incaricato di comunicare al Garante per la Protezione dei dati personali il *databreach,* per conto del Titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, informandone contestualmente il Data Protection Officer.

Il paragrafo 3 del citato articolo 35 specifica che:

> La notifica di cui al paragrafo 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.

Tutte le persone autorizzate al trattamento devono essere adeguatamente istruite affinché trattino correttamente i dati personali e informino, con la massima celerità, il Delegato di ogni violazione rilevata (*databreach*), affinché quest'ultimo possa procedere con le suddette segnalazioni.

6. Comunicazione di una violazione dei dati personali all'interessato

L'articolo 34 si occupa della questione della necessità di avvisare o meno l'interessato circa l'avvenuto *databreach*.
Ai sensi del GDPR, 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, elencate nel paragrafo 3 del citato articolo 34:

> 3. Non è richiesta la comunicazione all'interessato [...] 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, con l'assistenza della Direzione ICT e Agenda Digitale e la consulenza del Data Protection Officer, è tenuto ad effettuare l'istruttoria e provvedere a documentare le scelte effettuate, nonché - se nel caso - a comunicare la violazione all'Interessato.

7. Trattamenti effettuati con l'ausilio di strumenti elettronici

Nel caso di trattamenti di dati personali effettuati con strumenti elettronici, il Delegato dovrà adottare, per quanto di propria competenza, le misure tecniche di seguito indicate:

a) il trattamento di dati personali con strumenti elettronici è consentito solo alle "persone autorizzate", dotate di credenziali di autenticazione univoche. Il Delegato deve istruire le persone autorizzate sulla necessaria cautela da adottare per assicurare la segretezza e la custodia delle credenziali. Le predette credenziali di autenticazione non possono essere assegnate ad altre persone, neppure in tempi diversi.

> Le credenziali di autenticazione più diffuse sono la coppia: "identificativo/nome utente" e "password".

b) il Delegato determina le modalità organizzative per consentire comunque, in caso di prolungata assenza o impedimento della persona autorizzata al trattamento, la disponibilità dei dati, specie nei casi in cui all'assenza della predetta persona comporti un rallentamento non ammissibile per l'attività d'ufficio.

c) Il Delegato, prima dell'inizio del trattamento con l'utilizzo di applicativi, individua l'ambito del trattamento consentito alle singole persone autorizzate e richiede per la persona autorizzata l'attribuzione del "*profilo di autorizzazione*" adeguato all'ambito di trattamento consentito al medesimo.
Il Delegato deve inoltre verificare periodicamente la sussistenza delle condizioni per la conservazione del profilo di autorizzazione assegnato alla persona autorizzata. Il Delegato, definite o modificate le facoltà operative attribuite alla stessa, deve dare comunicazione tempestiva al *Call Center* dell'assistenza informatica per l'adeguamento del profilo (privilegi di accesso).

> I "profili di autorizzazione" sono l'insieme delle facoltà operative/operazioni, tecnicamente consentite dal sistema informatico/applicativo all'Incaricato, in relazione all'ambito di trattamento consentito al medesimo.

d) con riguardo alla protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici, il Delegato deve vietare alla persona autorizzata di comunicare ad altri le proprie credenziali nonché di usare le credenziali di altre persone autorizzate.
Il Delegato deve, altresì, ricordare ai lavoratori che non è consentita:

1) l'installazione di qualsiasi *software* che non sia debitamente autorizzato (*potendo l'installazione di un software alterare – indipendentemente dalla volontà dell'utilizzatore – la funzionalità delle postazioni di lavoro, sia sotto il profilo dell'integrità, disponibilità e riservatezza dei dati sia del collegamento in rete*);

2) la creazione e l'utilizzazione di "cartelle condivise", che contengano dati personali, senza l'impostazione nominativa della condivisione e senza l'eliminazione della voce "*everyone*" dalle "autorizzazioni condivisione" (*diversamente l'accesso alla cartella sarebbe incontrollato*).

e) limitatamente all'adozione di procedure per la custodia di copie di sicurezza ed il ripristino della disponibilità dei dati, il Delegato deve dare disposizioni affinché le persone autorizzate effettuino periodici *backup* dei dati personali. I supporti contenenti le eventuali copie di backup, atte al ripristino del sistema, devono essere custoditi accuratamente.

f) ricordato il principio di ***pseudonimizzazione*** (v. più sopra), per determinati trattamenti, in particolare per le "categorie particolari di dati", è necessario adottare tecniche di cifratura dei dati o codificazione degli interessati o delle informazioni.

Il Delegato, nel caso di specie, deve assicurarsi che i *software* utilizzati siano dotati di cifratura e di autenticazione forte (ad es. *smart card*).

8. Trattamenti effettuati senza l'ausilio di strumenti elettronici

Nel caso di trattamenti effettuati senza l'ausilio di strumenti elettronici, il Delegato al trattamento dovrà adottare le misure indicate di seguito.
Si precisa che le sotto indicate modalità di conservazione/custodia dei documenti dovranno essere applicate anche nell'ipotesi di copie/riproduzioni degli atti originali.

a) Il Delegato deve aggiornare, ogni qualvolta si renda necessario, l'individuazione dell'ambito del trattamento consentito (con supporti cartacei) alle singole persone autorizzate, affinché le medesime abbiano accesso ai soli dati la cui conoscenza sia necessaria per adempiere ai compiti loro assegnati.

b) Il Delegato impartisce alle persone autorizzate 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.
Quando gli atti e i documenti, contenenti particolari categorie di dati o relativi a condanne penali o reati, sono affidati alle persone autorizzate per lo svolgimento dei relativi compiti, il Delegato impartisce istruzioni affinché i medesimi atti e documenti siano controllati e custoditi dalle persone autorizzate, fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione e siano restituiti al termine delle operazioni affidate.

c) Il Delegato dispone che l'accesso ad archivi, contenenti particolari categorie di dati o relativi a condanne penali o reati, sia controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate.
Qualora gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.