Compiti
del
Responsabile del Trattamento

Regione del Veneto

AREA PROGRAMMAZIONE E SVILUPPO STRATEGICO

Direzione ICT e Agenda Digitale

Premessa

Si è da poco concluso a livello europeo il lungo percorso di approvazione del nuovo Regolamento generale sulla protezione dei dati: il "*Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", pubblicato nella Gazzetta Ufficiale dell'Unione Europea serie L 119 del 04.05.2016.
Tale Regolamento, di portata generale e obbligatorio in tutti i suoi elementi, sarà direttamente applicabile negli Stati membri dell'Unione europea a decorrere dal **25 maggio 2018**. Da quella data cesserà di avere efficacia il Decreto Legislativo 30 giugno 2003 n. 196 (Codice Privacy).
Risulta, pertanto, opportuno tener conto fin da subito di quanto indicato nel Regolamento (Ue) 2016/679.

PARTE PRIMA

TRATTAMENTO DEI DATI E COMPITI DEL RESPONSABILE

1. Definizioni e regole fondamentali.

Ai sensi dell'art. 4 del D.Lgs. 196/2003 si intende per:

a) "*trattamento*", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
b) "*dato personale*", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
c) "*dati sensibili*", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni ed organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
d) "*dati giudiziari*", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
e) "*dati comuni*", i dati personali che, per esclusione, non appartengono alle predette categorie dei dati sensibili o giudiziari.

Le strutture regionali possono trattare i dati personali "*comuni*" solo per svolgere le rispettive funzioni istituzionali *(art. 18, comma 2, del D.Lgs. 196/2003).*

Tale principio è confermato dal Regolamento (Ue) 2016/679 all'art. 6, par. 1, lett. e), laddove annovera tra le condizioni di liceità del trattamento: "*l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*";

Norme più stringenti, di seguito indicate al punto 5, disciplinano la comunicazione e la diffusione dei dati "*comuni*" (*art. 19, comma 2 e 3 del D.Lgs. 196/2003)*

Il trattamento dei dati sensibili o giudiziari, nondimeno, è consentito solo se è autorizzato da un'espressa disposizione di legge o di regolamento che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili sui dati medesimi e le finalità di rilevante interesse pubblico perseguite *(artt. 20 e 21 del D.Lgs. 196/2003).*

> Se il trattamento non è previsto espressamente da una disposizione di legge (nazionale o regionale) o di regolamento, esso è consentito solo se previsto dal Regolamento regionale n. 1 del 22 marzo 2007 e s.m.i. e nei limiti e nelle forme ivi stabilite.

Anche tale principio trova conferma nel nuovo Regolamento (Ue) 2016/679 all'art. 9, par. 2, laddove vengono annoverati tra le condizioni di liceità del trattamento i "*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*".

Quando il trattamento è direttamente disciplinato dalla normativa di settore, devono essere scrupolosamente osservati presupposti, limiti e modalità di trattamento, rinvenibili direttamente o desumibili dalla stessa, che rilevino ai fini del trattamento dei dati personali *(art. 18, comma 3, del D.Lgs. 196/2003).*

Il Responsabile del trattamento deve garantire la qualità dei dati, le corrette modalità di raccolta, conservazione e trattamento degli stessi, anche da parte del personale della propria struttura, secondo quanto disposto dal Codice Privacy, dai Provvedimenti del Garante e dal presente documento e vigila sul rispetto delle istruzioni impartite (**VERIFICA DEI TRATTAMENTI DI DATI**).

Le strutture regionali devono astenersi dal richiedere il consenso o un'autorizzazione al trattamento dei dati personali da parte degli Interessati *(art. 18, comma 4, del D.Lgs. 196/2003)* [1].
Il consenso è, infatti, richiesto solo da parte dei soggetti privati e degli enti pubblici economici, nonché in ambito sanitario, dagli organismi sanitari pubblici ed esercenti le professioni sanitarie (*artt. 18, comma 4, 23, 76 e ss. del D.Lgs. 196/2003*).

Si riporta di seguito, per completezza, l'art. 5, "*Principi applicabili al trattamento di dati personali*", del nuovo Regolamento (Ue) 2016/679:

> 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

[1] Una parziale deroga alla regola predetta è, nondimeno, accettata in materia di immagini e filmati per i quali si preveda la diffusione, in particolare nel caso di dati personali di minori.
Il nuovo Regolamento generale sulla protezione dei dati n. 2016/679, all'art. 8, prescrive che qualora il trattamento si basi sul consenso, " *il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale*".

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***»).

2. Organizzazione – sistema privacy.

Nell' "organizzazione - privacy" di Regione del Veneto le figure coinvolte sono:

1. il "*Titolare del trattamento*": è la "figura" di vertice cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza dei dati. Per i trattamenti di dati personali, effettuati dalle strutture regionali afferenti alla Giunta Regionale, titolare è la Giunta Regionale.
2. il "R*esponsabile (interno) del trattamento*": è un soggetto designato dal Titolare che, per esperienza, capacità ed affidabilità, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza. In Regione del Veneto il Responsabile del trattamento è generalmente individuabile nelle figure apicali, salvo limitate eccezioni. Lo si definisce anche Responsabile "*interno*" per distinguerlo dal Responsabile "*esterno*". Relativamente ai trattamenti di dati personali trasversali a più strutture, per l'individuazione si applica il criterio del maggiore ambito decisionale attribuito o vi possono essere situazioni di co-responsabilità.
3. il "*Responsabile esterno del trattamento*": è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo, esterno all'Amministrazione regionale, che, previa designazione formale del Responsabile "*interno*" del trattamento, assume (su delega di quest'ultimo) poteri decisionali su un determinato trattamento e deve attenersi, nelle operazioni svolte, alle istruzioni ricevute.
4. l' "*Amministratore di Sistema*": è, in ambito informatico, la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*Enterprise resource planning*), le reti locali e gli apparati di sicurezza, nella misura in cui tali attività di gestione e manutenzione consentano di intervenire sui dati personali.
5. l' "*incaricato del trattamento*" (persona autorizzata al trattamento): è la **persona fisica** che, operando sotto l'autorità del Responsabile, effettua le operazioni di trattamento dei dati, attenendosi alle istruzioni ricevute.
6. il "*Referente Privacy*": è il soggetto che, presso la struttura di appartenenza, coadiuva il Responsabile "*interno*" del trattamento e gli incaricati del trattamento nel disbrigo degli adempimenti in materia di privacy.
7. l' "*Interessato*": è la persona fisica cui si riferiscono i dati personali (sono escluse dal campo di applicazione della normativa privacy le persone giuridiche).

Il Responsabile del trattamento nomina, per iscritto, quali Incaricati del trattamento i propri collaboratori "*interni*" all'Amministrazione regionale (tipicamente il personale dipendente) (*art. 30 del D.Lgs. 196/2003*).

Il Responsabile del trattamento può nominare, per iscritto, quali Incaricati del trattamento, altresì, anche eventuali collaboratori "*esterni*" dell'Amministrazione (purché persone fisiche), a prescindere dal rapporto contrattuale intrattenuto con la stessa (ad es. stagisti, tirocinanti, ecc.), non dotati di potere decisionale autonomo, se stabilmente presenti negli uffici dell'Amministrazione.

Nella nomina degli Incaricati il Responsabile individua l'ambito del trattamento consentito ad ognuno, in base alle mansioni svolte, e impartisce **istruzioni scritte** per garantire che ciascun collaboratore tratti dati personali strettamente indispensabili per lo svolgimento dell'attività assegnatagli, nel pieno rispetto del Codice Privacy, delle presenti istruzioni e di quanto egli stesso ritenga necessario in base alla tipologia dei trattamenti dei dati effettuati dalla propria struttura. (**NOMINA INCARICATI DEL TRATTAMENTO**).

(*Nella pagina Intranet della Direzione ICT e Agenda Digitale – Ufficio Privacy è disponibile un modello – modificabile – di nomina*)

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 Responsabile del trattamento "*interno*" (ad es. avvocati "esterni", società di consulenza, ecc.), quest'ultimo deve provvedere a formalizzare la nomina di Responsabile "*esterno*" del trattamento (**NOMINA RESPONSABILE "ESTERNO"**).

(*Nella pagina Intranet della Direzione ICT e Agenda Digitale – Ufficio Privacy è disponibile un modello di nomina di responsabile esterno)*

Il Responsabile "*interno*" deve distinguere tra la nomina del Responsabile "*esterno*" e la nomina dell'Incaricato del trattamento, che opera sotto la sua diretta autorità. Di seguito si riporta una tabella riepilogativa:

COLLABORATORI del Responsabile "interno"	**Interni**	**Esterni**	
		(non dotati di potere decisionale autonomo)	*(dotati di potere decisionale autonomo)*
Persona fisica	Nomina ad Incaricato *(tipicamente il personale dipendente)*	Nomina ad Incaricato (*ad es. stagisti, tirocinanti, ecc.)*	Designazione Responsabile Esterno *(ad es. avvocati "esterni", ecc.)*
Persona giuridica	---	---	Designazione Responsabile Esterno *(ad es. società di consulenza, ecc.)*

Se al soggetto esterno è affidata l'amministrazione di sistemi informatici, esso deve essere investito dal Responsabile "*interno*" anche del compito di "Amministrazione dei Sistemi", ai sensi del Provvedimento del Garante del 27.11.2008 sugli Amministratori di Sistema.

Al fine di garantire un efficace "*sistema privacy*" regionale, il Responsabile del trattamento individua all'interno della propria struttura un "*Referente Privacy*" che si interfaccia con la Direzione ICT e Agenda Digitale – Ufficio Privacy per l'analisi delle questioni che interessano la struttura di appartenenza.
Il nominativo ed ogni successiva sostituzione del Referente devono essere tempestivamente comunicati alla Direzione ICT e Agenda Digitale (**COMUNICAZIONE REFERENTE PRIVACY**), indicando nella comunicazione anche il Codice Struttura e il Nome struttura:

Codice struttura	Nome struttura	Nome e cognome del Referente Privacy	Telefono Ufficio

3. Informativa.

Gli Interessati hanno il diritto di ricevere un'idonea e preventiva Informativa circa modalità e soggetti Responsabili del trattamento dei loro dati personali *(art. 13 del D.Lgs. 196/2003)*:

L'interessato, o la persona presso la quale sono raccolti i dati personali, sono previamente informati per iscritto circa:
a) quali sono le finalità e quali sono le modalità del trattamento (informatizzate e/o cartacee) cui sono destinati i dati;
b) la natura obbligatoria (*base giuridica del trattamento*) o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito eventuale di diffusione dei dati medesimi (indicando altresì la norma di legge che autorizza la diffusione);
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del Titolare e del Responsabile del trattamento, indicando il recapito a cui l'interessato può rivolgersi per l'esercizio dei diritti di cui al punto precedente.

Tale adempimento, anche per ragioni di opportunità ed economia organizzativa, deve essere svolto nel momento in cui ciascuna struttura raccolga i dati personali (con compilazione di *brochure* o *format on line*, etc.) e non va rinviato a tempi successivi (risulta gravoso a posteriori raggiungere ogni Interessato per notificare l'Informativa).

Il Responsabile del trattamento informa, per iscritto, l'Interessato ovvero la persona presso la quale sono raccolti i dati personali, degli elementi previsti dall'art. 13 del Codice Privacy, prima dell'inizio del trattamento. (**INFORMATIVA**).

In calce all'Informativa può essere richiesta una firma all'interessato esclusivamente "*per presa visione*" e non come autorizzazione/consenso al trattamento (vedi sopra).

Sul punto, il Regolamento (Ue) 2016/679, all'art. 13, conferma quanto già previsto dall'art. 13 del Codice Privacy e aggiunge, quale elemento di novità obbligatorio dal 25 maggio 2018, l'indicazione del "*periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo*" e "*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*".

(*Nella pagina Intranet della Direzione ICT e Agenda Digitale – Ufficio Privacy è disponibile un modello di Informativa da completare)*

4. Videosorveglianza

Per quanto riguarda la videosorveglianza, il Responsabile del trattamento delle immagini riprese e/o registrate con le telecamere deve rispettare gli obblighi di legge previsti dallo Statuto dei Lavoratori nonché il Provvedimento Generale sulla Videosorveglianza del Garante Privacy dell'8 aprile 2010, curando altresì l'affissione degli appositi cartelli, recanti l'Informativa con l'immagine della telecamera, nonché l'aggiornamento delle informazioni in essi indicate.
Il Responsabile dell'impianto di videosorveglianza deve, altresì, designare per iscritto tutte le persone fisiche incaricate del trattamento ed i livelli di autorizzazione all'accesso alle immagini.
Qualora il Responsabile ("interno") si avvalga di manutentori/società esterni, questi devono essere nominati Responsabili "esterni"del trattamento.

5. Comunicazione e diffusione dei dati. Pubblicazione di atti.

La comunicazione di dati personali da parte di una struttura regionale ad altre Pubbliche Amministrazioni (*effettuata in qualunque forma, anche previa convenzione, ed in assenza di nomina del Responsabile "esterno"*) è ammessa quando è prevista da una norma di legge o di regolamento.
In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è stata data previa informazione (tramite PEC) al Garante Privacy delle circostanze e motivazioni per cui si intende effettuare la comunicazione ad altra Pubblica Amministrazione ed il Garante Privacy non si è espresso in senso contrario entro 45 giorni dal ricevimento della predetta comunicazione (*art. 19, comma 2, del D.Lgs. 196/2003)*

La comunicazione di dati personali da parte di una struttura regionale a privati o a enti pubblici economici, invece (*in assenza di nomina del Responsabile "esterno"*) e la diffusione di dati personali sono ammesse unicamente quando sono previste da una norma di legge o di regolamento. (*art. 19, comma 3, del D.Lgs. 196/2003)*

Ai sensi del D.Lgs. 196/2003 si distinguono:
1) "*comunicazione*", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
   Lo scambio di dati tra strutture afferenti alla Giunta Regionale non costituisce "comunicazione" e nemmeno lo scambio di dati tra una struttura regionale ed il Responsabile "esterno" (formalmente designato dal Responsabile "interno").
2) "*diffusione*", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
   La principale forma di "diffusione" è data dalla pubblicazione di dati personali, direttamente o contenuti in atti e documenti, nel sito *web* dell'Amministrazione regionale e nei siti tematici dell'Amministrazione regionale.

Per quanto riguarda la pubblicazione di atti e documenti contenenti dati personali e/o la divulgazione di dati personali attraverso i siti internet dell'Amministrazione regionale, poiché queste azioni determinano una "diffusione" di dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di cittadini, devono essere adottate opportune cautele riguardo i dati personali pubblicati.
L'interferenza nella sfera personale degli Interessati, che consegue a tale pubblicazione, è legittima solo se la predetta diffusione è prevista da una norma di legge o di regolamento *(artt. 4, comma 1, lett. m), e 19, comma 3, del D.Lgs. 196/2003).*
E' quindi fondamentale che fin dalla stesura dei provvedimenti destinati alla pubblicazione, si valuti con estrema attenzione la necessità o meno di inserire dati personali e la tipologia degli stessi.

La responsabilità correlata al rispetto degli artt. 19, comma 3, 20 e 21 del D.Lgs. 196/2003, relativi alla diffusione di dati personali, è imputabile esclusivamente alle strutture che hanno redatto gli atti e documenti contenenti dati personali e/o hanno proceduto con la divulgazione di dati personali attraverso i siti internet dell'Amministrazione regionale (ad es. la piattaforma di pubblicazione del BURVET, la sezione "Amministrazione trasparente", ecc.).

Sul tema si possono consultare le "*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*" [doc. web n. 3134436] del 15 maggio 2014. Tali Linee Guida forniscono utili esemplificazioni.

Non devono essere in alcun caso diffuse *on line* o riportate negli atti pubblicati nel *web*, informazioni idonee a rivelare lo stato di salute degli interessati (*artt. 22, comma 8, e 68, comma 3, del D.Lgs. 196/2003*).

Si pensi, in tale ultimo caso, all'indicazione:
- dei titoli dell'erogazione dei benefici (es. attribuzione di borse di studio a "*soggetto portatore di handicap*", o riconoscimento di buono sociale a favore di "*anziano non autosufficiente*" o con l'indicazione, insieme al dato anagrafico, delle specifiche patologie sofferte dal beneficiario);
- dei criteri di attribuzione (es. punteggi attribuiti con l'indicazione degli "*indici di autosufficienza nelle attività della vita quotidiana*");
- della destinazione dei contributi erogati (es. contributo per "*ricovero in struttura sanitaria oncologica*").

Alcuni adempimenti di legge, in capo al Titolare – Giunta Regionale, richiedono la necessaria collaborazione di tutte le strutture con la Direzione ICT e Agenda Digitale - Ufficio Privacy che svolge attività di consulenza e coordinamento (**PARTICOLARI ADEMPIMENTI DI LEGGE**).

Ad esempio, dal 25 maggio 2018, la compilazione del nuovo Registro delle Attività (Re.d.A.) di trattamento effettuate presso le varie strutture (art. 30 del nuovo Regolamento europeo 2016/679).

6. Diritto d'accesso ai dati personali

Gli Interessati hanno diritto di accedere ai propri dati *(art. 7 del D.Lgs. 196/2003)*.
Il Responsabile deve fornire il riscontro all'Interessato si è rivolto "senza ritardo" e comunque entro il termine di 15 giorni (30 giorni se la ricerca è complessa). (**DIRITTO D'ACCESSO DELL'INTERESSATO ED ALTRI DIRITTI**).

L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

PARTE SECONDA

SICUREZZA E COMPITI DEL RESPONSABILE

1. Principi generali sulla sicurezza dei dati

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

Il D.lgs. 196/2003, agli artt. da 33 a 36, nonché l'Allegato B del D.Lgs. 196/2003, indicano, nel quadro dei più generali obblighi di sicurezza di cui all'art. 31, le misure minime di sicurezza da adottare nel trattamento dei dati personali.

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, come più ampiamente descritto di seguito.

Rientra, in ogni caso, nei compiti del Responsabile l'adozione di ulteriori e più adeguate misure di sicurezza, ritenute necessarie per la particolare tipologia dei dati trattati e della modalità del trattamento.

Il Regolamento (UE) 2016/679 nel 39° "considerando iniziale", precisa che: "*onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. 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*".

Al fine di accrescere la consapevolezza in materia di sicurezza informatica, il Responsabile del trattamento promuove la diffusione e l'utilizzo delle procedure definite dal documento "*Regole Comportamentali per gli Utenti nell'uso delle risorse ICT dell'Amministrazione regionale*" (Allegato B alla Delibera che approva il presente documento) all'interno della struttura che dirige, vigilando ed assicurando che i sistemi, i dati e le applicazioni siano utilizzati in conformità ai criteri definiti nel suddetto documento. (**CONSAPEVOLEZZA DELLA SICUREZZA INFORMATICA**)

2. Censimento patrimonio informativo, banche dati e *databreach.*

Ogni Responsabile del trattamento ed ogni Incaricato 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 Responsabile del trattamento cura periodicamente il censimento delle Banche Dati e dei trattamenti di dati personali effettuati dalla struttura che dirige. (**CENSIMENTO**)

Per gli incidenti che coinvolgano dati personali (cd. "***databreach***") il Garante per la Protezione dei dati personali è intervenuto con il documento: "*Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015*" [doc. web. 4129029].
Per ottemperare agli obblighi imposti da tale documento ogni Responsabile del trattamento avvisa tempestivamente la Direzione ICT e Agenda Digitale di tutte le violazioni dei dati o gli incidenti informatici che possono avere un impatto significativo sui dati personali contenuti nelle banche dati di propria competenza. Il Responsabile segnalante, assieme alla Direzione ICT e Agenda Digitale,

comunica al Garante per la Protezione dei dati personali, entro 48 ore dalla conoscenza del fatto, dell'avvenuto incidente di ***databreach.*** (**SEGNALAZIONE DEI DATABREACH**).

> Il Regolamento (UE) 2016/679 al 85° "considerando" iniziale precisa che:
> "*… non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe* ***notificare la violazione*** *dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo ….*"
>
> Al 86° "considerando" iniziale, inoltre, aggiunge che:
> "*Il titolare del trattamento dovrebbe* ***comunicare all'interessato la violazione*** *dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. ...*"
>
> L'87° "considerando" iniziale, infine, precisa che:
> "*È opportuno verificare se siano state* ***messe in atto tutte le misure tecnologiche e organizzative adeguate*** *di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato…*"

Il Regolamento (UE) 2016/679, inoltre, all'art. 30 prevede che ogni Titolare/Responsabile del trattamento tenga obbligatoriamente dal 25 maggio 2018 un **Registro delle attività** di trattamento effettuate sotto la propria responsabilità.
Tale registro verrà messo a disposizione dell'Autorità Garante per la Protezione dei dati personali in caso di esplicita richiesta e/o di sopralluogo.

3. Trattamenti effettuati con l'ausilio di strumenti elettronici

Nel caso di trattamenti di dati personali effettuati con strumenti elettronici, il Responsabile del trattamento dovrà adottare le misure minime indicate dalla lettera a) alla lettera h) di cui all'art. 34 D.Lgs. 196/2003 (meglio specificate nell'Allegato B al predetto decreto legislativo), per quanto di propria competenza, delle quali di seguito si fornisce una sintetica esplicitazione:

a) il trattamento di dati personali con strumenti elettronici è consentito solo agli "Incaricati", dotati di credenziali di autenticazione univoche. Il Responsabile deve istruire gli Incaricati sulla necessaria cautela da adottare per assicurare la segretezza e la custodia delle credenziali. Le predette credenziali di autenticazione non possono essere assegnate ad altri Incaricati, neppure in tempi diversi.
(Art. 34, comma 1, lett. a) del D.Lgs. 196/2003).

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

b) il Responsabile determina le modalità organizzative per consentire, in caso di prolungata assenza o impedimento dell'Incaricato, la disponibilità dei dati e degli strumenti elettronici ad esso assegnati promuovendo l'individuazione, direttamente da parte del lavoratore interessato dall'assenza, di un "*delegato fiduciario*" che acceda a tutte le risorse necessarie in sua assenza.
(Art. 34, comma 1, lett. b) del D.Lgs. 196/2003).

> Il "*delegato fiduciario*" è una figura particolarmente funzionale laddove le credenziali di autenticazione, consentano l'accesso a "Banche dati", documenti ed applicazioni per lo svolgimento delle funzioni istituzionali e la cui mancata fruizione, dovuta all'assenza dell'Incaricato, comporti un rallentamento non ammissibile per l'attività amministrativa.

L'accesso, resosi necessario in caso di assenza dell'Incaricato impone al Responsabile di informare tempestivamente lo stesso Incaricato dell'intervento effettuato, avvalendosi delle credenziali depositate presso il "*delegato fiduciario*".
Tale ultima figura di "*delegato fiduciario*" è peraltro espressamente prevista dal "*Disciplinare per l'utilizzo di Posta elettronica, internet, Telefoni e fax all'interno di Regione del Veneto*" (Allegato alla DGR n. 863/2009) con riferimento alla regolamentazione regionale per l'accesso del Direttore alla posta elettronica del dipendente assente, cui si rinvia per maggiori dettagli.

c) Il Responsabile, prima dell'inizio del trattamento con l'utilizzo di applicativi, individua l'ambito del trattamento consentito ai singoli Incaricati e richiede per l'incaricato l'attribuzione del "*profilo di autorizzazione*" adeguato all'ambito di trattamento consentito al medesimo.
Il Responsabile deve inoltre verificare periodicamente la sussistenza delle condizioni per la conservazione del profilo di autorizzazione assegnato all'Incaricato. Il Responsabile, definite o modificate le facoltà operative attribuite allo stesso, deve dare comunicazione tempestiva al *Call Center* per l'adeguamento del profilo (privilegi di accesso).
(*Art. 34, comma 1, lett. c) e lett. d) del D.Lgs. 196/2003*)

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 Responsabile deve vietare all'Incaricato di comunicare ad altri le proprie credenziali nonché di usare le credenziali di altri Incaricati, salvo quanto disposto alla precedente lett. b).
Il Responsabile 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*);

3) 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*).

(*Art. 34, comma 1, lett. e) del D.Lgs. 196/2003*).

e) limitatamente all'adozione di procedure per la custodia di copie di sicurezza ed il ripristino della disponibilità dei dati, il Responsabile deve dare disposizioni affinché gli Incaricati effettuino periodici *backup* dei dati personali. I supporti contenenti le eventuali copie di backup, atte al ripristino del sistema, devono essere custoditi accuratamente.
(*Art. 34, comma 1, lett. f) del D.Lgs. 196/2003*).

f) per determinati trattamenti, relativi a dati idonei a rivelare lo stato di salute o la vita sessuale (ad es. banche dati sanitarie), è necessario adottare tecniche di cifratura dei dati o codificazione degli interessati o delle informazioni.
Il Responsabile, nel caso di specie, deve assicurarsi che i *software* utilizzati siano dotati di cifratura e di autenticazione forte (ad es. *smart card*).
(*Art. 34, comma 1, lett. h) del D.Lgs. 196/2003*).

4. Trattamenti effettuati senza l'ausilio di strumenti elettronici

Nel caso di trattamenti effettuati senza l'ausilio di strumenti elettronici, il Responsabile del trattamento dovrà adottare, nei modi previsti dal disciplinare tecnico contenuto nell'Allegato B del D.Lgs. 196/2003, le misure indicate all'art. 35, delle quali di seguito di fornisce una sintetica esplicitazione.
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 Responsabile deve aggiornare, con cadenza almeno annuale, l'individuazione dell'ambito del trattamento consentito (con supporti cartacei) ai singoli incaricati, affinché gli incaricati abbiano accesso ai soli dati la cui conoscenza sia necessaria per adempiere ai compiti loro assegnati.
La lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione, nelle modalità previste dall'art. 30, comma 2, del D.Lgs. 196/2003.
(*Art. 35, comma 1, lett. a) del D.Lgs. 196/2003*).

b) Il Responsabile del trattamento impartisce agli Incaricati 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 dati personali sensibili o giudiziari, sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti, il Responsabile impartisce istruzioni affinché i medesimi atti e documenti siano controllati e custoditi dagli Incaricati, fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione e siano restituiti al termine delle operazioni affidate.
(*Art. 35, comma 1, lett. b) del D.Lgs. 196/2003*).

c) Il Responsabile dispone che l'accesso ad archivi contenenti dati sensibili o giudiziari 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.
(*Art. 35, comma 1, lett. c) del D.Lgs. 196/2003*).