Regolamento per l'attuazione del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

CISIS - Centro Interregionale per i Sistemi Informatici, Geografici e Statistici
Via Piemonte, 39 - 00187 Roma - Codice fiscale 96184870580

INDICE

CAPO I – DISPOSIZIONI GENERALI

Articolo 1 – Oggetto

1. Il presente regolamento disciplina le misure organizzative ed i processi interni in materia di trattamento dei dati personali delle persone fisiche nell'ambito delle funzioni e finalità istituzionali del Centro Interregionale per i Sistemi informatici, geografici e statistici, di seguito denominato CISIS, in attuazione del Regolamento europeo (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"*, (di seguito anche "GDPR o Regolamento europeo") e del D.Lgs.30 giugno 2003, n. 196 *"Codice in materia di protezione dei dati personali"*, (di seguito anche "Codice"), modificato dal D.Lgs.10 agosto 2018, n. 101, recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"*.

2. Ai fini del presente regolamento, si intendono per funzioni istituzionali:

- le funzioni previste dalla legge, dallo Statuto del CISIS, dai regolamenti e dalla normativa comunitaria;
- le funzioni svolte per mezzo di intese, accordi di programma e convenzioni nelle materie di competenza del CISIS.

Articolo 2 – Finalità del trattamento

1. I dati personali sono trattati dal CISIS, nel rispetto dei principi sanciti dall'art. 5 del Regolamento (UE) 2016/679, per le seguenti finalità istituzionali:

a) l'adempimento di un obbligo legale al quale è soggetto l'Ente in qualità di Titolare del trattamento;

b) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

- l'esercizio delle funzioni istituzionali (amministrative, tecniche, di ricerca) indicate nello statuto del CISIS, ovvero al fine di perseguire lo scopo di promuovere e garantire un efficace coordinamento tra le Regioni e le Province autonome di Trento e di Bolzano per la definizione, lo sviluppo ed il coordinamento di iniziative e attività inerenti alla Società dell'informazione e della conoscenza e per assicurare il miglior raccordo tra le Regioni, lo Stato e gli Enti Locali su tali temi;

- l'esercizio delle attività di competenza dell'Area tecnica ed in particolare dell'Area Sistemi Informatici, dell'Area Sistemi Geografici e dell'Area Sistemi Statistici;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale, regionale, provinciale, attribuite all'Ente in base alla vigente legislazione;

c) l'esecuzione *ex lege* di un contratto o misure precontrattuali con gli interessati;

d) specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento dei propri dati personali.

Art. 3 – Ambito di applicazione

1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in uno o più archivi o destinati a figurarvi del CISIS.

2. Il presente regolamento non si applica ai trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse ai sensi dell'art. 2, paragrafo 2, lett. d), del Regolamento (UE) 2016/679; per detti trattamenti trova applicazione il D.Lgs. 18 maggio 2018 n. 51 recante *"Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio"*.

Articolo 4 – Definizioni

1. Ai fini del presente regolamento s'intende per:

Interessato: è tale la persona fisica identificata o identificabile in base ai dati personali trattati;

dato personale: qualsiasi informazione riguardante l'**interessato**; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di

messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

trattamento su larga scala: trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti;

profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

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;

titolare del trattamento: il CISIS, in persona del suo legale rappresentante (Presidente o, in sua assenza, Vice Presidente *pro-tempore*), ovvero, 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;

contitolare del trattamento: due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali;

responsabile del trattamento: i Settori rappresentati organicamente dal loro Dirigente, ovvero, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Per il CPSI il Responsabile dell'Area Tecnica dei Sistemi Informativi; per il CPSG il Responsabile dell'Area Tecnica dei Sistemi Geografici; per il CPSS il Responsabile dell'Area Tecnica dei Sistemi Statistici;

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 Europea 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;

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;

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;

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;

dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento (UE) 2016/679 ovvero il Garante per la protezione dei dati personali;

rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

D.P.I.A.: è la "Valutazione di Impatto sulla Protezione dei Dati" ovvero quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati particolare, o anche per una combinazione di questi e altri fattori), il Regolamento (UE) 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti , cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato;

Codice: il Decreto Legislativo 30 giugno 2003 n. 196 recante il "Codice in materia di protezione dei

dati personali", modificato dal Decreto Legislativo 10 agosto 2018, n. 101;

GDPR o Regolamento Europeo: il *"General Data Protection Regulation"*, ovvero, il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (regolamento generale sulla protezione dei dati).

CAPO II - SOGGETTI DEL TRATTAMENTO

Articolo 5 – Titolare del trattamento

1. Il Titolare del trattamento dati è il CISIS, in persona del suo legale rappresentante *pro-tempore* (di seguito indicato anche "Titolare").

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'articolo 5 del Regolamento (UE) 2016/679:

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

3. La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del Regolamento europeo. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento europeo. Dette misure sono riesaminate e aggiornate qualora necessario.

4. Le misure sono definite fin dalla fase di progettazione e messe in atto per ridurre al minimo il trattamento dei dati personali e applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

5. Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'articolo 13 del GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'articolo 14 del GDPR, qualora i dati personali non sono stati ottenuti presso lo stesso interessato.

6. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "D.P.I.A.") ai sensi dell'articolo 35 e ss. del GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

7. Il Titolare provvede a:

a) designare i Responsabili del trattamento dati, individuati:

- nei Comitati Permanenti dell'Ente, rappresentati organicamente dal Responsabile dell'Area Tecnica dei Sistemi Informativi, dei Sistemi Geografici e dei Sistemi Statistici;
- nei soggetti pubblici o privati, affidatari di attività e servizi per conto del titolare, relativamente alle banche dati gestite da soggetti esterni all'Ente, in virtù di convenzioni, contratti, incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali; per dette designazioni il Titolare autorizza direttamente i Comitati Permanenti dell'Ente;

b) nominare il Responsabile della protezione dei dati (RPD-DPO) *ex* art. 37 e ss. del GDPR.

8. Il titolare del trattamento deve verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare dall'art. 28, paragrafo 3, del Regolamento europeo.

9. Il titolare del trattamento deve valutare l'esistenza di eventuali situazioni di contitolarità, essendo obbligato in tal caso a stipulare l'accordo interno di cui all´art. 26, paragrafo 1, del GDPR.

Articolo 6 – Contitolari del trattamento

1. La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.

2. Nell'ambito dell'esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al CISIS dai soci aderenti, da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'articolo 26 del GDPR.

3. Il CISIS e i suoi soci aderenti sono da considerarsi, pertanto, ognuno per le proprie rispettive attribuzioni *ex* artt. 13 e 14 D.Lgs. 18 agosto 2000, n. 267, nonché per effetto di convenzioni ed accordi, Titolari o Contitolari del trattamento dei dati personali.

4. L'accordo di contitolarità:

a) definisce le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento Europeo, con particolare riferimento all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando quanto eventualmente stabilito dalla normativa specificatamente applicabile;

b) può designare un punto di contatto comune per gli interessati;

c) riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato, ai fini dell'esercizio dei diritti previsti dagli articoli 15 e ss. del GDPR. Indipendentemente dalle disposizioni di tale accordo, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.

Articolo 7 – Responsabile del trattamento

1. Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

2. Il Titolare si avvale di Responsabili individuati nei Responsabili delle Aree Tecniche dei sistemi Informativi, Geografici e Statistici in virtù di specifico contratto/convenzione.

3. Il Responsabile del trattamento, che tratta i dati personali per conto del Titolare del trattamento, deve rispettare pienamente quanto previsto dalle leggi vigenti e dalle disposizioni del regolamento europeo in materia di trattamento e sicurezza dei dati personali.

4. Il Responsabile del trattamento procede alla designazione degli **incaricati** ovvero delle **persone autorizzate al trattamento** dei dati personali che si impegnano alla riservatezza e che assumono pertanto un obbligo legale di riservatezza. La nomina delle persone autorizzate al trattamento avviene mediante atto scritto, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.

La nomina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun responsabile designato.

5. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'articolo 28 del Regolamento (UE) 2016/679.

6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

7. Il Regolamento europeo consente la nomina di **sub-responsabili** del trattamento da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile "primario"; le operazioni di trattamento possono essere effettuate solo da persone autorizzate che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificamente l'ambito del trattamento consentito.

8. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, in particolare:

- alla tenuta del registro delle attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- ad assistere il Titolare nella conduzione della D.P.I.A. fornendo allo stesso ogni informazione di cui è in possesso;
- in caso di violazione dei dati personali ad informare il Titolare, senza ingiustificato ritardo, ed in ogni caso entro 24 ore dal momento in cui ne è venuto a conoscenza (cd. *"data breach"*), per consentire al Titolare la notificazione al Garante per la protezione dei dati personali, entro i termini previsti dall'art. 33, comma 1, del Regolamento (UE) 2016/679, ovvero, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Articolo 8 - Responsabile della protezione dati

1. Il Titolare del Trattamento procede alla nomina del Responsabile della protezione dei dati (RPD-DPO) *ex* art. 37 e ss. del GDPR. Il Titolare o il Responsabile del trattamento provvede alla pubblicazione dei dati di contatto del DPO ed alla comunicazione del nominativo al Garante per la protezione dei dati personali in conformità all'articolo 37, paragrafo 7, del Regolamento. Questa disposizione mira a garantire che

l’autorità di controllo possa contattare il Responsabile della Protezione dei Dati in modo facile e diretto. In base all'articolo 39, paragrafo 1, lettera e), del GDPR, il Responsabile della Protezione dei Dati funge da punto di contatto fra l’Ente e il Garante.

2. Il R.P.D. è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il R.P.D. può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, ed a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare sull’osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l’analisi e la verifica dei trattamenti in termini di loro conformità, l’attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla D.P.I.A. e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il R.P.D. in merito a:

- se condurre o meno una D.P.I.A.;
- quale metodologia adottare nel condurre una D.P.I.A.;
- se condurre la D.P.I.A. con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
- se la D.P.I.A. sia stata condotta correttamente o meno e se le conclusioni raggiunte siano conformi al GDPR;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all’articolo 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del R.P.D. è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) verificare la tenuta dei registri delle attività e delle categorie di trattamento, sotto la responsabilità del Titolare del trattamento.

3. Il Titolare ed il Responsabile del trattamento assicurano che il R.P.D. sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il R.P.D. è invitato a partecipare alle riunioni di coordinamento che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il R.P.D. deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del R.P.D. sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta dall'Ente determini condotte difformi da quelle raccomandate dal R.P.D., è necessario motivare specificamente tale decisione;
- il R.P.D. deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

4. Il R.P.D. è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, che il Titolare potrà garantire, compatibilmente con le risorse di Bilancio, qualora la disciplina dello specifico rapporto preveda tale tipo d'intento, con onere di comunicazione di detto adempimento al Titolare ed al Responsabile del trattamento.

5. Nello svolgimento dei compiti affidatigli il R.P.D. deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il R.P.D.:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività-, incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

6. Il R.P.D. dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

7. La figura di R.P.D. è incompatibile con chi determina le finalità od i mezzi del trattamento. In particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;
- qualunque incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.

8. Il Titolare ed il Responsabile del trattamento forniscono al R.P.D. le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al

R.P.D.:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili amministrativi;
- tempo sufficiente per l'espletamento dei compiti affidati al R.P.D.;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero tramite la costituzione di una U.O., ufficio o gruppo di lavoro R.P.D. (formato dal R.P.D. stesso e dal rispettivo personale);
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

9. Il Responsabile della protezione dati:

a) opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. In particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati;

b) non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il R.P.D. riferisce direttamente al Titolare od al Responsabile del trattamento.

10. Nel caso in cui siano rilevate dal R.P.D. o sottoposte alla sua attenzione decisioni incompatibili con il Regolamento Europeo, con altre norme dell'ordinamento e/o con le indicazioni fornite dallo stesso R.P.D., quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

CAPO II - SICUREZZA DEL TRATTAMENTO

Articolo 9 - Sicurezza del trattamento

1. L'art. 5, par. 1, lett. f), del Regolamento (UE) 2016/679 stabilisce che i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza degli stessi, compresa la protezione, mediante misure tecniche e organizzative adeguate, a garanzia degli obblighi di integrità e disponibilità dei dati. Tale obbligo è richiamato negli articoli 24, 28 e da 32 a 34 del Regolamento europeo e tale valutazione sarà rimessa, caso per caso, al titolare, contitolare e al responsabile, in rapporto ai rischi specificamente individuati dall'art. 32 del regolamento europeo, tenendo conto dei seguenti elementi:

- lo stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità

del trattamento, come anche 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, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale;

- la notificazione della violazione dei dati nel rispetto delle tempistiche previste dagli artt. 33 e 34 del GDPR e la comunicazione all'interessato, senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

2. Il rischio per i diritti e le libertà delle persone fisiche inerente al trattamento, costituisce uno degli elementi da considerare per valutare l'adeguatezza delle misure tecniche ed organizzative. Le Linee Guida del *Gruppo di Lavoro Articolo 29*, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017, concernenti *"la valutazione di impatto nonché i criteri per stabile se il trattamento possa presentare un rischio elevato"*, precisano che per "rischio" s'intende uno scenario descrittivo di un evento e delle relative conseguenze che sono stimate in termini di gravità e probabilità. 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.

3. 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.

4. L'adeguatezza delle misure di sicurezza deve ricomprende, pertanto, tra le altre, se del caso:

a) l'adozione di tecniche di 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.

5. Il titolare e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare, poiché costituisce una misura di sicurezza anche l'istruzione delle persone autorizzate al trattamento, ai sensi dell'art. 32, paragrafo 4, del Regolamento europeo.

Articolo 10 - Registri delle attività di trattamento

1. I registri di trattamento sono raccolti su strumento di archiviazione telematico, secondo le indicazioni dettate dalla normativa vigente.

2. L'art. 30 del GDPR dispone, infatti, l'obbligo per ogni titolare e responsabile del trattamento di tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

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

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

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

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

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, paragrafo 1, del Regolamento (UE) 2016/679.

3. Su richiesta, il titolare del trattamento o il responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Articolo 11 - Valutazioni d'impatto sulla protezione dei dati

1. La Valutazione d'impatto sulla protezione dei dati (D.P.I.A.) è un processo previsto nei casi di trattamento che prevede l'uso di nuove tecnologie o quando trattasi di trattamento di nuovo tipo e per i quali il titolare del trattamento non ha ancora effettuato alcuna DPIA, o quando l'esecuzione della D.P.I.A. sia necessaria alla luce del tempo trascorso dal trattamento iniziale.

2. Gli articoli 35 e 36 del GDPR prevedono che, quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento stesso, possa presentare un rischio elevato per i diritti e le persone fisiche, il titolare del trattamento proceda, prima di effettuare il trattamento stesso, alla predisposizione della D.P.I.A.

3. Il Titolare del trattamento:

a) è responsabile dello svolgimento di una preventiva D.P.I.A. per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione deve essere preso in considerazione nella determinazione delle opportune misure tecniche ed organizzative da adottare per dimostrare che il trattamento dei dati personali rispetta il regolamento europeo;

b) sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento, nei casi in cui la D.P.I.A. riveli la presenza di rischi residui elevati che non possono essere attenuati mediante l'adozione di misure opportune per la riduzione del rischio a livello accettabile. La consultazione preventiva è assoggettata al rispetto delle disposizioni di cui all'art. 36.

4. Ai sensi degli artt. 35, par. 4, e 57, par. 1, lett. k), del GDPR, fermo restando quanto indicato nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati", il Garante per la protezione dei dati personali ha individuato, con Provvedimento n. 467 dell'1 ottobre 2018, l' "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679",* soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto. L'elenco è il seguente:

1. Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on- line o attraverso app, relativi ad "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 dell'interessato.

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "*effetti giuridici*" oppure che incidono "*in modo analogo significativamente*" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere.

3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

4. Trattamenti su larga scala di dati aventi carattere estremamente personale così come disciplinati dalle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati" adottate dal Gruppo di Lavoro Art. 29; in particolare si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata o che incidono sull'esercizio di un diritto fondamentale oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato, quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti.

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti, così come dettagliato nelle Linee guida sopra riportate.

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili, quali ad esempio minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo.

7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo, quali ad esempio IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad esempio il *wi-fitracking*, ogni qualvolta ricorra anche almeno un altro dei criteri individuati nelle Linee guida sopra riportate.

8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento, quali ad esempio il *mobile payment*.

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 del GDPR oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Tale elenco è riferito esclusivamente a tipologie di trattamento soggette al meccanismo di coerenza e non è esaustivo, restando fermo quindi l'obbligo di adottare una D.P.I.A. laddove ricorrano due o più dei criteri individuati in materia dalle Linee guida del Gruppo di Lavoro Art. 29 e che in taluni casi "un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno dei predetti criteri richieda una valutazione d'impatto sulla protezione dei dati".

5. Il Titolare:

- garantisce l'effettuazione della D.P.I.A. ed è responsabile della stessa;
- può affidare la conduzione materiale della D.P.I.A. ad un altro soggetto, interno o esterno all'Ente;
- deve consultarsi con il R.P.D. anche per assumere la decisione di effettuare o meno la D.P.I.A. Tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della D.P.I.A;
- può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati;
- deve procedere alla consultazione preventiva del Garante per il trattamento dei dati personali, prima di procedere al trattamento, se le risultanze della D.P.I.A. condotta indicano l'esistenza di un rischio residuale elevato, che non è stato attuato neppure a fronte dell'adozione di misure tecniche ed organizzative adeguate;
- consulta il Garante Privacy nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

6. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della D.P.I.A. fornendo ogni informazione necessaria.

7. Il Responsabile della protezione dati (R.P.D.-D.P.O.) monitora lo svolgimento della D.P.I.A. e può proporre lo svolgimento di una D.P.I.A. in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

8. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una dichiarazione relativa all'effettuazione della D.P.I.A.

Articolo 12 - Violazione dei dati personali

1. La violazione dei dati personali è definita come la *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati"* dal Titolare o dal Responsabile del trattamento (art. 4, n. 12, Regolamento (UE) 2016/679). Al riguardo si definiscono le seguenti tipologie:

- *distruzione:* si ha "distruzione" di dati personali quando non esistono più o non esistono più in una forma che possa essere di qualsiasi utilità per il Titolare;
- *perdita:* il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento ha perso il controllo o l'accesso oppure non ha più il possesso;
- "danno": si verifica quando i dati personali sono stati alterati, corrotti o non sono più completi;
- *trattamento non autorizzato o illecito:* il "trattamento non autorizzato o illecito" può includere la divulgazione di dati personali a (o accesso da parte di) destinatari che non sono autorizzati a ricevere (o accedere a) i dati, o qualsiasi forma di trattamento che viola il Regolamento.

2. In caso di violazione dei dati personali, il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, ha l'obbligo di notificare la violazione (c.d. *"data breach"*) al Garante per la protezione dei dati personali, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo (art. 33 GDPR).

3. Il Responsabile del trattamento in caso di violazione dei dati personali è obbligato ad informare il Titolare, senza ingiustificato ritardo ed in ogni caso entro 24 ore dal momento in cui ne è venuto a conoscenza (cd. *"data breach"*), per consentire al Titolare la notificazione all'Autorità di Controllo entro i termini previsti dall'art. 33, comma 1, del Regolamento (UE) 2016/679, ovvero, entro 72 ore dal momento in cui ne è venuto a conoscenza.

4. La notifica 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.

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

6. 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.

7. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al GDPR, sono i seguenti (*a titolo non esaustivo*):

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

8. Se il Titolare ritiene che il rischio per i diritti e le libertà delle persone fisiche ovvero degli interessati conseguente alla violazione rilevata è elevato, allora deve informare, -salvo i casi riportati al comma 8 del presente articolo-, questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. La comunicazione agli interessati deve contenere almeno le informazioni e le misure di cui al paragrafo 4,

lettere b), c) e d), del presente articolo, ai sensi dell'art. 34 del GDPR.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi;
- comportare rischi imminenti e con un'elevata probabilità di accadimento, quali ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito;
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni, quali ad esempio utenti deboli, minori, soggetti indagati.

9. 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;

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.

10. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al precedente comma 8 è soddisfatta.

11. Il Titolare deve opportunamente e comunque documentare le violazioni di dati personali subite, anche se non comunicate all'autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante per la protezione dei dati personali al fine di verificare il rispetto delle disposizioni del Regolamento (UE) 2016/679.

12. Tali disposizioni sono ulteriormente analizzate nelle Linee Guida adottate dal Gruppo di Lavoro

Articolo 29 in data 3 ottobre 2017 ed approvate nella versione emendata il 6 febbraio 2018.

13. Il Titolare del trattamento adotterà un Registro dei casi di *data breach*, in cui verranno annotati i casi di violazione effettivamente occorsi e le minacce potenziali, e ciò al fine di identificare il tipo e la natura delle violazioni più ricorrenti.

14. Il tracciamento dei casi di violazione dei dati personali verrà effettuato allo scopo di:

- individuare e tenere sotto controllo i fattori di rischio, ossia i fattori che determinano con più frequenza una violazione dei dati personali;
- misurare l'efficacia delle *policy* e delle procedure adottate;
- elaborare un piano di conformità che fissi gli obiettivi da raggiungere per essere *"compliant"* rispetto a leggi, *best practices*, e che aiuti a dimostrare la conformità in sede di audit di verifica/ispezioni/test.

Per gestire e risolvere i casi di *data breach* l'Ente si avvale principalmente della propria struttura, secondo gli ambiti di propria competenza, potendo ricorrere a soluzioni esterne nei casi di particolare complessità e qualora risulti necessario acquisire professionalità non in dotazione all'Ente stesso.

Articolo 13 Rinvio

1. Per tutto quanto non espressamente previsto e disciplinato con il presente regolamento, si applicano le disposizioni del Regolamento europeo, leggi e regolamenti vigenti e le Linee guida approvate dal "Gruppo Art. 29" per la protezione dei dati personali.