

# Policy per la gestione delle ispezioni da parte del Garante per la protezione dei dati personali

## Sommario

<u>1. INTRODUZIONE</u> .....	50
<u>1.1 Scopo ed obiettivi</u> .....	50
<u>1.2 Ambito di applicazione</u> .....	50
<u>2. DEFINIZIONI</u> .....	51
<u>3. QUADRO NORMATIVO DI RIFERIMENTO</u> .....	52
<u>3.1 Riferimenti normativi e regolamentari</u> .....	52
<u>4. TEAM PER LA GESTIONE DELLE ISPEZIONI</u> .....	53
<u>5. LA GESTIONE DELLE ISPEZIONI</u> .....	53
<u>5.1 Le Ispezioni del Garante</u> .....	53
<u>5.2 Indicazioni di carattere generale relative alle Ispezioni in loco</u> .....	54
<u>5.3 Il ruolo del DPO nella gestione della Ispezioni</u> .....	54
<u>6. PROCESSO PER LA GESTIONE DELLE ISPEZIONI</u> .....	55
<u>6.1 Processo</u> .....	55
<u>6.1.1 Analisi della richiesta e coinvolgimento dei soggetti competenti</u> .....	55
<u>6.1.2 Predisposizione contributi per rispondere alla richiesta</u> .....	55
<u>6.1.3 Predisposizione e formalizzazione della risposta</u> .....	55
<u>7. DOCUMENTAZIONE RILEVANTE</u> .....	56
<u>8. CONSEGUENZE DELLE ISPEZIONI</u> .....	57
<u>8.1 Ricorso giustizia ordinaria avverso il provvedimento del garante</u> .....	57
<u>8.2 Azioni successive</u> .....	59

---

<sup>1</sup> Allegato aggiunto dall'articolo 12, comma 1, del r.r. 4 aprile 2025, n. 8, pubblicato sul BUR Lazio 8 aprile 2025, n. 28.

## 1. INTRODUZIONE

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 - *Regolamento generale sulla protezione dei dati* (GDPR) prevede che tutti i titolari del trattamento sono tenuti a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente allo stesso Regolamento (art. 24, par. 1, GDPR).

Il Regolamento contempla tra i principi applicabili alla protezione dei dati personali anche l'*accountability* (responsabilizzazione) dei titolari e responsabili del trattamento (art. 5, par. 1, GDPR), consistente nell'adozione di comportamenti proattivi, tali da provare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

In conformità al predetto principio è attribuita al Titolare la "responsabilità generale" del trattamento e l'attuazione di un sistema organizzativo e gestionale che preveda misure reali, efficaci e comprovabili di protezione dei dati (v. Cons. 74 e artt. 5, par. 2, e 24 del GDPR).

Tale approccio implica, oltre alla corretta e puntuale predisposizione degli adempimenti imposti dalla normativa in tema di protezione dei dati, anche l'implementazione di procedure e prassi organizzative atte a conformare i trattamenti al GDPR.

Il Regolamento contempla altresì l'obbligo generale di cooperazione con l'Autorità di controllo da parte del Titolare e responsabile del trattamento (art. 31 e Cons. 82 del GDPR).

La presente policy descrive le procedure relative alla gestione delle ispezioni del Garante per la protezione dei dati personali.

Nell'esercizio dei suoi compiti di controllo il Garante per la protezione dei dati personali (di seguito anche "Autorità" o "Garante"), valutati gli elementi in suo possesso, anche in assenza di reclami, segnalazioni o notificazioni di violazione dei dati personali, può avviare d'ufficio accertamenti per verificare la sussistenza di elementi in ordine a possibili violazioni in materia di protezione dei dati personali.

L'attività ispettiva può essere curata dal dipartimento, servizio o altra unità organizzativa del Garante competente in materia di attività ispettive e di revisione ovvero delegata alla Guardia di Finanza. La stessa può essere altresì effettuata avvalendosi, ove necessario, della collaborazione di altri organi dello Stato.

La programmazione dell'attività ispettiva di iniziativa viene approvata dal Garante su base semestrale con propria deliberazione.

Gli accertamenti, di seguito anche "Ispezioni", possono verificarsi in due modalità:

- istruttoria cartolare;
- accesso ai locali.

### 1.1 Scopo ed obiettivi

La presente policy descrive le modalità e le fasi per gestire gli eventuali accertamenti ispettivi da parte del Garante per la protezione dei dati personali da parte della Giunta regionale del Lazio (di seguito "Giunta" o "Titolare"), nella sua qualità di Titolare o, quando ricorra la fattispecie, di Responsabile del trattamento, ai sensi del GDPR e del D. Lgs. 196/2003 e ss.mm.ii. (di seguito "Codice in materia di protezione dei dati personali" o anche solo "Codice").

## 1.2 Ambito di applicazione

La presente Policy si applica alla Giunta e al suo personale, secondo le responsabilità e i ruoli previsti all'interno del modello organizzativo per la protezione dei dati personali di cui al Titolo IX, Capo V del Regolamento Regionale n.1/2002 e successive modifiche.

## 2.DEFINIZIONI

Di seguito si riportano le definizioni dei termini utilizzati nella presente Policy.

TERMINE	DESCRIZIONE
<b>Dato Personale</b>	<i>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 (art. 4 par. 1 GDPR).</i>
<b>Trattamento</b>	<i>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 (art 4 par. 2 GDPR).</i>
<b>Interessato</b>	<i>La persona fisica alla quale i dati personali si riferiscono (vedasi la definizione di Dato Personale).</i>
<b> Titolare del trattamento</b>	<i>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 (art 4 par. 7 RGDP).</i>
<b> Responsabile del trattamento</b>	<i>La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art 4 par. 8 GDPR).</i>
<b> Contitolari del trattamento</b>	<i>La contitolarità si verifica quando due o più soggetti definiscono congiuntamente le finalità e i mezzi del trattamento (art. 26 GDPR).</i>
<b> Autorizzato al trattamento</b>	<i>La persona fisica che effettua materialmente le operazioni di trattamento sui dati personali e che opera alle dipendenze del Titolare e/o del Responsabile (art. 29 GDPR e art. 2 quaterdecies del Codice).</i>
<b> DPO (Data Protection Officer)</b>	<i>Soggetto incaricato dal Titolare o dal Responsabile del trattamento per assolvere a funzioni di supporto e di controllo, consultive, formative e informative, di attribuzione delle responsabilità relativamente all'applicazione del GDPR (Art. 37 GDPR).</i>
<b> Categorie particolari di dati personali</b>	<i>Dati personali che possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in</i>

TERMINE	DESCRIZIONE
	<i>modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (Art. 9 GDPR).</i>
<b>Misure di sicurezza</b>	<i>Le misure tecniche e organizzative predisposte dal Titolare o dal Responsabile di trattamento ai sensi dell'Art. 32 GDPR.</i>
<b>Amministratori di sistema</b>	<i>Figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti ai sensi del Provvedimento del Garante della Privacy del 27 novembre 2008 recante prescrizioni ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema.</i>
<b>Registro dei trattamenti</b>	<i>E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del GDPR) relative alle operazioni di trattamento svolte dal Titolare e, se nominato, dal responsabile del trattamento. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.</i>
<b>DPIA (Data protection Assessment) (Data Impact)</b>	<i>E' una procedura prevista dall'articolo 35 del GDPR che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.</i>

### 3. QUADRO NORMATIVO DI RIFERIMENTO

#### 3.1 Riferimenti normativi e regolamentari

La presente Policy tiene conto delle disposizioni contenute nelle seguenti norme nazionali ed europee:

- Regolamento (UE) 2016/679 in materia di protezione dei dati personali, (in breve "RGPD", meglio conosciuto con l'acronimo inglese "GDPR");
- D.lgs. n. 196/2003 ("Codice in materia di protezione dei dati personali");  
in particolare:
  - Art. 58 del GDPR "Poteri";
  - Art. 83 del GDPR "Condizioni generali per infliggere sanzioni amministrative pecuniarie";
  - Considerando 122, 129 e 132 del GDPR;
  - Parte III, Titolo II, Capo III del Codice in materia di protezione dei dati personali;
  - Art. 157 del Codice "Richiesta di informazioni e di esibizione dei documenti";
  - Art. 158 del Codice "Accertamenti";
  - Art. 31 GDPR "Cooperazione con l'Autorità di Controllo".
- e nei seguenti ulteriori atti e regolamenti:
  - Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali approvato con Deliberazione del 4 aprile 2019 del Garante;
  - Programmazione dell'attività ispettiva di iniziativa, curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, approvata su base semestrale con deliberazione dell'Autorità;

- Regolamento 1/2000 concernente l'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali.

#### 4. TEAM PER LA GESTIONE DELLE ISPEZIONI

Per far fronte alle ispezioni da parte dell'Autorità la Giunta, in qualità di Titolare del Trattamento, opera per il tramite di un apposito Team preposto all'assistenza dell'attività ispettiva, costituito come segue:

Codice	Attore
SDC	Soggetto Designato competente nelle materie oggetto dell'attività ispettiva.
SDP	Soggetto Designato competente in materia di dati personali
DG	Direttore Generale
DPO	DPO
AR	Avvocatura regionale

#### 5. LA GESTIONE DELLE ISPEZIONI

##### 5.1 Le Ispezioni del Garante

Le Ispezioni del Garante sono volte a verificare che le attività di trattamento dei dati personali di una determinata organizzazione siano conformi alla normativa vigente in ambito protezione dei dati personali. Le Ispezioni possono scaturire da segnalazioni o reclami da parte degli Interessati, oppure su iniziativa del Garante sulla base dell'attività ispettiva programmata su base semestrale con propria deliberazione.

Le Ispezioni possono distinguersi secondo le seguenti tipologie:

1. **Ispezioni tramite istruttoria cartolare** nell'ambito delle quali il Garante può richiedere al Titolare e/o Responsabile di fornire ogni informazione necessaria per l'esecuzione dei suoi compiti (art. 58 par. 1 lett. a) GDPR). L'istruttoria cartolare può precedere anche l'ispezione tramite accesso ai locali.
2. **Ispezioni tramite accesso presso i locali del Titolare e/o Responsabile** (Art. 58 par. 1 lett. f) GDPR). L'ispezione presso i locali può avvenire:
  - o con preavviso tramite una comunicazione via PEC (posta elettronica certificata) o residualmente via raccomandata A/R, anche il giorno prima dell'arrivo dei soggetti preposti all'ispezione;
  - o senza preavviso.

Il perimetro dell'Ispezione è individuato all'interno del documento che viene notificato dall'Autorità tramite PEC, in caso di istruttoria cartolare, o al momento dell'accesso nei locali della Giunta, in caso di Ispezione presso i locali.

La supervisione semestrale del piano ispettivo dell'Autorità, finalizzata alla conoscenza degli argomenti sui quali il Garante programma la propria attività ispettiva e la sua divulgazione a tutte le strutture regionali, è demandata alla Direzione Regionale competente in materia di protezione dei dati personali per il tramite del Direttore *pro tempore* nella qualità di soggetto designato.

Di seguito sono descritte le modalità di gestione delle Ispezioni.

##### 5.2 Indicazioni di carattere generale relative alle Ispezioni in loco

Ai fini del buon esito delle Ispezioni, la Giunta opera per mezzo del Team di cui al precedente par. 4; il SDC competente nelle materie e nei trattamenti oggetto dell'ispezione, per tutta la durata

dell'Ispezione stessa coordina le attività e costituisce il punto di riferimento per le strutture regionali coinvolte e per gli ispettori.

Durante l'attività ispettiva il SDC può farsi assistere da consulenti di propria fiducia e riservarsi di produrre la documentazione non immediatamente reperibile entro un termine congruo.

Gli Ispettori raccolgono presso il SDC tutta la documentazione relativa al perimetro ispettivo stabilito, nonché l'ulteriore documentazione utile ai fini della dimostrazione della *compliance* alla normativa in materia di protezione dati personali da parte dello stesso.

In particolare, il personale ispettivo può:

- richiedere informazioni o spiegazioni;
- accedere alle banche dati e agli archivi;
- controllare, estrarre ed acquisire copia dei documenti, anche in formato elettronico.

Per una più dettagliata identificazione della documentazione che può essere richiesta e sottoposta a controllo durante l'Ispezione si rinvia al paragrafo 7 della presente Policy.

Della veridicità delle dichiarazioni rese dal Titolare del trattamento, e dal suo personale autorizzato, nel corso dell'istruttoria, si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice Privacy.

Al termine di ciascuna giornata di ispezione, il SDC si assicura di far registrare nel verbale di ispezione dell'Autorità le proprie considerazioni o dichiarazioni in particolare se in contrasto con le valutazioni emerse durante l'attività ispettiva da parte del Garante.

Il SDP redige un report interno per documentare le attività svolte e ove possibile quelle programmate per la giornata successiva, allegando copia del verbale delle Autorità. Il report ha lo scopo di tenere traccia degli uffici visitati, dei dipendenti interrogati e dei documenti consegnati durante l'ispezione, in modo da poter ricostruire accuratamente i dettagli delle Ispezioni.

### 5.3 Il ruolo del DPO nella gestione della Ispezioni

Tra i compiti del DPO, ai sensi dell'art. 39 del GDPR, vi è quello di "cooperare con l'autorità di controllo" e "fungere da punto di contatto con l'autorità". Inoltre, l'articolo 38 del GDPR prevede che "*il Titolare del trattamento e il responsabile del trattamento assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".

Il DPO assiste il Titolare durante le ispezioni. In particolare, ne presidia tutte le fasi e funge da punto di contatto per facilitare l'accesso, da parte dell'Autorità Garante, ai documenti e alle informazioni necessarie per l'adempimento dei compiti ad essa attribuiti dall'art. 57, nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'art. 58 del GDPR.

## 6. PROCESSO PER LA GESTIONE DELLE ISPEZIONI

L'accesso ai locali della Giunta da parte del personale incaricato dall'Autorità, nonché la comunicazione dell'Autorità della visita ispettiva in loco o di istruttoria cartolare, sono immediatamente comunicate al SDP, il quale procede ad informare il DPO e a convocare il Team come sopra costituito.

### 6.1 Processo

#### 6.1.1 Analisi della richiesta e coinvolgimento dei soggetti competenti

<b>R</b>	<b>A</b>	<b>C</b>	<b>I</b>
SDP	SDP	TEAM	TEAM

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Sia in caso di istruttoria cartolare che in caso di Ispezione in loco, il SDP, in primo luogo provvede a informare il DPO il quale si occuperà di presidiare ogni fase del processo di Ispezione. In seguito, l'SDP prende visione del provvedimento ricevuto, ne esamina attentamente il contenuto e attiva tempestivamente il Team coinvolto nella gestione dell'Ispezione. Qualora le materie oggetto di Ispezione riguardino le competenze di più Soggetti Designati, il DG nomina il SDC di riferimento.

Il SDP, ove le verifiche riguardino i sistemi informativi, coinvolge il Responsabile del trattamento, il quale con l'atto di nomina si è impegnato ad adottare tutte le misure tecniche indicate dall'art. 32 del RGPD.

### 6.1.2 Predisposizione contributi per rispondere alla richiesta

R	A	C	I
SDC	SDC	SDP/AR	DPO/DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Una volta attivato il Team, l'SDC raccoglie tutta la documentazione e le informazioni utili alla predisposizione dei riscontri al Garante.

Ai fini del riscontro nei termini stabiliti dall'Autorità, nelle ispezioni in loco, nonché nelle istruttorie cartolari il SDC predispose la documentazione richiesta; qualora ciò implichi di fornire l'accesso a documenti cartacei ed elettronici il SDC è supportato in particolare dal SDP e dall'AR.

### 6.1.3 Predisposizione e formalizzazione della risposta

R	A	C	I
SDC	SDC	SDP/AR/DPO	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Nell'istruttoria cartolare, il SDC, con il supporto del DPO, del SDP e dell'AR, informato il DG, formalizza la risposta e provvede all'invio nei termini stabiliti dall'Autorità.

Nell'Ispezione in loco, il SDC revisiona la lista dei documenti forniti, le minute, i commenti e le osservazioni sollevate durante l'attività ispettiva e nell'ipotesi di istruttorie particolarmente complesse o richieste di documentazione articolate o di particolare rilevanza può valutare, coadiuvato dal DPO e dall'AR e dal SDP, la richiesta di un differimento dei termini all'Autorità, verificando all'occorrenza con gli stessi eventuali punti ancora da chiarire.

## 7. DOCUMENTAZIONE RILEVANTE

La tabella che segue evidenzia una serie di documenti utili a dimostrare la *compliance* con la normativa in materia di protezione dei dati personali, generalmente oggetto di richiesta da parte del Garante in caso di ispezione, nonché il rispetto del principio di *accountability*.

In considerazione del fatto che il GDPR prevede in tema di protezione e trattamento dei dati personali che le attività poste in essere siano adeguatamente documentate, la documentazione

relativa a eventuali *Assessment* svolti in materia, deve essere conservata al fine di renderla disponibile per dimostrare la conformità delle attività di trattamento ai principi normativi vigenti in materia.

La conservazione, compatibilmente con le dotazioni in essere presso la Giunta, deve essere effettuata in un apposito *repository*.

<b>Elenco documenti</b>
Accordi sindacali e/o autorizzazioni della DTL (direzione territoriale del lavoro)
Regolamento Regionale CAPO V “ <i>Trattamento dei dati personali e banche dati</i> ” nell’ultima versione disponibile
Autorizzazione al trattamento del soggetto incaricato ai sensi dell’art. 29 del Regolamento 2016/679/UE e dell’art. 2 quaterdecies del D. lgs. 196/03 e istruzioni operative
Designazione di amministratore di sistema ai sensi del provvedimento del Garante per la protezione dei dati personali (G.U. n. 300 del 24/12/2008)
Nomina del DPO
Evidenze relative all’attività di formazione per i dipendenti
Designazione Responsabili del trattamento (DPA)
Documentazione di <i>assessment</i> Privacy (es. <i>checklist</i> GDPR)
Documentazione sui sistemi informatici utilizzati (verifiche/ <i>assessment</i> )
Documentazione Videosorveglianza (es. accordo sindacale)
Valutazione del rischio delle attività di trattamento
DPIA svolte, complete, ove esistenti degli aggiornamenti
Elenco Amministratori di Sistema e relative nomine
Elenco eventuali contitolari e relativi accordi di contitolarità
Elenco responsabili/sub-responsabili del trattamento
Informative e modulistica standard
Misure di sicurezza adottate
Procedure specifiche in materia di protezione e trattamento dei dati personali (es. per esercizio diritti interessati)
Registro attività di trattamento tenuti in qualità di Titolare e/o Responsabile del trattamento
<i>Data breach policy</i>
Registro <i>data breach</i>
<i>Repository</i> di segnalazioni e reclami avvenuti
Lista delle richieste di esercizio dei diritti pervenute
<i>Checklist</i> di controllo e esiti audit sulle attività dei Responsabili

Con particolare riferimento alle Ispezioni in loco, il Team, secondo le competenze sopra individuate si assicura di:

- rilasciare sempre informazioni veritiere e corrette;

- non rilasciare mai documentazione in originale ma solo in copia;
- prendere nota, nel report giornaliero di cui al paragrafo 4.2, di tutti i documenti (inclusi anche banche dati, archivi, software) visionati dagli ispettori e delle informazioni richieste e fornite;
- farsi rilasciare copia del verbale di ispezione dell’Autorità.

Qualora il riscontro alle richieste degli Ispettori costituisca attività di particolare complessità, sia in ordine all’istruttoria, sia in ordine al reperimento della documentazione richiesta, il SDC, informati il DPO e il DG, potrebbe valutare la richiesta di differimento dei termini al Garante.

## 8. CONSEGUENZE DELLE ISPEZIONI

R	A	C	I
SDC	SDC	DPO/AR	DG/DPO/SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Alla luce delle risultanze ispettive, il Garante, valutata la sussistenza di eventi di particolare rilevanza, può irrogare le sanzioni pecuniarie di cui all’art. 83 GDPR e/o i provvedimenti correttivi di cui all’art. 58 paragrafo 2 del GDPR.

Entro trenta giorni dalla comunicazione il SDC, coadiuvato dal DPO e dall’Avvocatura Regionale, informato il DG, può esercitare il proprio diritto di difesa inviando scritti difensivi e deduzioni scritte e può chiedere, con specifica istanza debitamente motivata una breve proroga, di norma concessa per un termine non superiore a quindici giorni, anche tenendo conto delle caratteristiche operativo/dimensionali del Titolare.

### 8.1 Ricorso giustizia ordinaria avverso il provvedimento del garante

R	A	C	I
SDC	SDC	AR	DPO/DG/SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Ai sensi del combinato disposto degli artt. 78 del Regolamento e 152 del d.lgs 196/2003 è prevista la possibilità di presentare ricorso avverso le decisioni dell’Autorità Garante davanti al Giudice ordinario, il quale può rideterminare le sanzioni irrogate dalla stessa Autorità Garante.

Nel caso di emissione della sanzione da parte dell’Autorità, spetta al SDC coadiuvato dall’AR e informati il DG e il DPO, la facoltà di proporre ricorso avverso il provvedimento sanzionatorio emesso dall’Autorità Garante innanzi alle Autorità giurisdizionali competenti, ai sensi dell’art. 78 del GDPR.

Tali controversie sono regolate dal rito del lavoro e vengono decise dal Tribunale ordinario in composizione monocratica, con sentenza non appellabile ma ricorribile unicamente tramite ricorso per Cassazione.

Il ricorso avverso i provvedimenti dell'Autorità, ivi compresi quelli emessi a seguito di un reclamo dell'interessato, è proposto, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Il Regolamento ha previsto rilevanti sanzioni di natura amministrativa in caso di violazioni della normativa sulla protezione dei dati personali. L'art. 83 del Regolamento distingue due gruppi di sanzioni amministrative.

Nel primo gruppo rientrano le violazioni cosiddette di minore gravità, per le quali sono previste le sanzioni amministrative pecuniarie di importi fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e comprendono, tra l'altro anche le violazioni degli obblighi imposti al Titolare e al Responsabile del trattamento (artt. 8, 11, da 25 a 39, 42 e 43 del GDPR).

Nel secondo gruppo rientrano le violazioni di maggiore gravità per le quali sono previste sanzioni pecuniarie fino all'ammontare di 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e riguardano nello specifico le seguenti violazioni:

- dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 del Regolamento;
- dei diritti degli interessati a norma degli articoli da 12 a 22 del Regolamento;
- delle norme relative ai trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli artt. da 44 a 49 del Regolamento;
- di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX del GDPR;
- nonché l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'Autorità Garante ai sensi dell'art. 58, par. 2 del Regolamento, o il negato accesso nella Società/Ente in violazione dell'art. 58, par. 1 del Regolamento.

Le sanzioni irrogate dall'Autorità devono essere effettive, proporzionate e dissuasive (art. 83, par. 1 del Regolamento) e devono tenere conto delle circostanze di cui all'art. 83, par. 2 del Regolamento, che contemplano anche il grado di cooperazione con l'Autorità al fine di porre rimedio alle rilevate violazioni; la modalità con cui il Titolare risponde alle richieste dell'Autorità durante le ispezioni, può costituire elemento di valutazione del grado di cooperazione con l'Autorità.

## 8.2 Azioni successive

All'esito del procedimento ispettivo, il SDC è tenuto a mettere in atto tutte le azioni correttive richieste dal provvedimento dell'Autorità, nonché ad adeguare la documentazione alle risultanze ispettive intervenendo sul sistema di protezione dati per apportare gli opportuni miglioramenti. Tutta la documentazione relativa all'Ispezione, comprensiva del verbale di ispezione, dei report interni di cui al paragrafo 4.2 nonché degli interventi di adeguamento documentati sul sistema di protezione dati deve essere adeguatamente conservata, compatibilmente con le dotazioni in essere presso la Giunta, anche in un apposito *repository*.”

