Provvedimento dell'11 giugno 2026 [10266034]

VEDI ANCHE Newsletter del 29 luglio 2026

[doc. web n. 10266034]

Provvedimento dell'11 giugno 2026

Registro dei provvedimenti
n. 426 dell'11 giugno 2026

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia, componente, e il dott. Luigi Montuori, segretario generale;

VISTO 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" (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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" (di seguito "Codice");

VISTO il 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 n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore il prof. Pasquale Stanzione;

PREMESSO

1. Introduzione.

In data 1° aprile 2025, la Provincia di Sassari, a cui è subentrata la Città Metropolitana di Sassari, ha notificato all'Autorità una violazione di dati personali ai sensi dell'art. 33 del Regolamento,

rappresentando di aver appreso, in data 26 marzo 2025, di un “eventuale accesso non autorizzato dipendente da cause organizzative”, riguardante il “gestionale protocollo e/o gestionale documentale residenti su server dell'Amministrazione”, che consente a “una platea di utenti (circa 30) con privilegi informatici […di] visualizzare sia il registro di protocollo sia i documenti allegati a ciascuna singola registrazione”, potendo, così, accedere a dati personali di “dipendenti/consulenti”. Ciò specificando che la violazione, che avrebbe avuto luogo dal 25 marzo al 29 marzo 2025, ha riguardato “n. 1 interessati”, in relazione a una “comunicazione del Commissario Liquidatore verso il Segretario Provinciale con richiesta di avvio di eventuale procedimento disciplinare a carico [di un Dirigente]”, con potenziale “pregiudizio alla reputazione” dello stesso.

A fronte di tale violazione, la Città Metropolitana dichiarava che erano state impartite “disposizioni del DPO tese a limitare il novero dei soggetti con livelli di privilegio idonei a consentire la consultazione di atti il cui livello di riservatezza è impostato al grado superiore possibile. In altri termini il livello di consultazione massimo è stato riservato alle figure apicali dell'Ente con richiesta di riorganizzazione delle utenze e dei relativi privilegi in base agli incarichi attribuiti”. Ciò tramite “articolazione dei privilegi di visione impostati sulle postazioni delle figure apicali con conseguente assegnazione dei protocolli secondo un'articolazione per servizi e uffici direttamente disposta dal Dirigente di ciascun settore secondo le micro organizzazioni interne e in coerenza con i profili di autorizzati al trattamento rispetto al personale assegnato”. In data 22 aprile 2025, la Città Metropolitana ha integrato la predetta notifica di violazione di dati personali, facendo presente che la violazione è stata resa nota all’interessato in data 22 aprile 2025.

Con successivo reclamo presentato ai sensi dell’art. 77 del Regolamento, la dott.ssa XX, Dirigente della Città Metropolitana, ha lamentato una presunta violazione della disciplina in materia di protezione dei dati personali, in relazione al medesimo fatto oggetto della predetta notifica di violazione dei dati personali e, dunque, con riguardo alla stessa nota riservata (prot. n. XX del XX), protocollata senza i necessari requisiti di riservatezza.

La reclamante, avvedutasi della problematica, informava il Responsabile della protezione dei dati (RPD) della Città Metropolitana che “nel settore da [ella] diretto già due operatori […] hanno fatto presente di aver potuto visionare e scaricare (con visibilità 9 utilizzata per protocollare la nota [in questione])”.

2. L’attività istruttoria.

In riscontro a una richiesta d’informazioni (v. nota prot. n. 0072629 del 28 maggio 2025), formulata dall’Autorità ai sensi dell’art. 157 del Codice, la Città Metropolitana, con nota del 17 giugno 2025 (prot. n. 0001504), ha dichiarato, in particolare, per il tramite del RPD, che:

- “con nota mail del XX la [reclamante], Dirigente […] della Città Metropolitana di Sassari […] comunicava […] una presunta violazione di dati, avvenuta mediante la protocollazione con piena visibilità del file allegato, di una comunicazione qualificata come riservata che, come accertato in seguito, ha ad oggetto e contenuto dati relativi ad ipotizzati profili di responsabilità disciplinare, spedita dall’ex Commissario Straordinario della ex Provincia di Sassari […] ed indirizzata al Segretario Generale […] in forma visibile a tutti gli operatori in possesso di un profilo di autorizzazione di tipo “9””;

- “in data 28/03/2025 […] il [RPD della Città Metropolitana] impartiva disposizioni organizzative e tecniche preordinate a garantire la conformità dei trattamenti […] onde evitare l'ulteriore protrarsi del rischio di una visibilità indiscriminata di tutti i protocolli qualificati come "riservati" di procedere con una disabilitazione dei privilegi estesi a tutto l'Ente […]”; in particolare, il RPD chiedeva che “tutte le utenze, ad esclusione delle figure apicali, responsabili dei sistemi o della protocollazione, dovranno avere abilitazione al livello

5” e suggeriva che “contestualmente potrà procedersi con una nuova definizione dei livelli di accesso strutturando le utenze in modo da attenersi all'organizzazione dell'Ente secondo la sequenza Dirigenti-Settori-Servizi-Uffici, così da far coincidere le abilitazioni agli utenti in coerenza con le microstrutture dei settori e le attribuzioni, operate dai Dirigenti con propria Determinazione, di addetto al trattamento dei dati”;

- “in data 28/03/2025 […] il Settore I forniva indicazioni su come riorganizzare la gestione degli accessi al protocollo e, più in dettaglio, per quello che rileva, chiedeva l’autorizzazione a modificare i privilegi di accesso precedentemente configurati in capo a lavoratori in grado di poter consultare l’intero protocollo con profilo da 9 a 5 (a prescindere da mansioni, compiti ed ufficio/servizio di assegnazione)”;

- “con mail del 28 marzo 2025 [… veniva adottate] disposizioni di servizio in ordine all’adeguamento dei profili di autorizzazione per l’accesso al protocollo informatico dell’Ente alle indicazioni formulate dal DPO”;

- “in data 02/04/2025 (prot. GPDP n. 44383) […] il [titolare] provvedeva a notiziare [l’] Autorità circa un’ipotesi di violazione di dati ai sensi delle disposizioni di cui all’art. 33 del Regolamento”.

Con una successiva nota del 17 luglio 2025 (prot. n. 0005993), a scioglimento di una riserva di ulteriori approfondimenti, precedentemente formulata, la Città Metropolitana, per il tramite del proprio RPD, ha prodotto in atti copia della corrispondenza intercorsa tra il RPD e talune articolazioni interne all’Ente in relazione ai fatti oggetto di reclamo.

A fronte di ulteriori chiarimenti chiesti dall’Autorità (v. nota prot. 0149338 dell’11 novembre 2025), la Città Metropolitana, con nota del 5 dicembre 2025 (prot. n. 2025/0024887), ha dichiarato che “non è possibile disporre delle informazioni relative agli specifici soggetti che abbiano acceduto alla nota prot. n. XX del XX, a causa dell'indisponibilità delle copie di back up relative ai file di log”.

Con nota del 30 marzo 2026 (prot. n. 0048990), l’Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell’attività istruttoria, ha notificato alla Città Metropolitana, ai sensi dell’art. 166, comma 5, del Codice, l’avvio del procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2, del Regolamento: per aver omesso, nel configurare il proprio protocollo informatico, di dare attuazione ai principi di protezione dei dati, con particolare riguardo a quelli di “integrità e riservatezza”, “responsabilizzazione” e “protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”, con conseguente violazione degli art. 5, parr. 1, lett. f), e par. 2, e 25 del Regolamento; per aver dato luogo, in ragione della scorretta configurazione del proprio protocollo informatico, a comunicazioni di dati personali a soggetti terzi non autorizzati al trattamento, con conseguente violazione degli artt. 5, par. 1, lett. a) e 6, par. 1, lett. c) ed e), del Regolamento e 2-ter del Codice, nonché, in relazione ai dati personali appartenenti a categorie particolari o relativi a reati, degli artt. 9 e 10 del Regolamento e 2-sexies e 2-octies del Codice. Con la medesima nota, il predetto titolare è stato invitato a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall’Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

Con nota del 30 aprile 2026 (prot. n. 0013531), la Città Metropolitana ha presentato una memoria difensiva, dichiarando, in particolare, che:

- “l'operatività dell'utente […] viene […] regolata attraverso una serie di abilitazioni specifiche articolate su tre livelli: la visibilità al registro, la visibilità alla sezione e la visibilità ai singoli corrispondenti, ciascuna espressa con un valore numerico da 1 a 9”;

- “poiché l'Ente dispone di un unico registro e di un'unica sezione, tutti gli utenti - ad

eccezione della visibilità più ampia consentita agli amministratori di modulo (Responsabili Settore 1) e al profilo per gli addetti al protocollo, sono abilitati al registro generale e alla sezione generale con visibilità di livello 4";

- "tale impostazione ha la funzione di circoscrivere la visibilità dei protocolli ai soli corrispondenti espressamente abilitati per ciascun utente, secondo una convenzione interna che prevede il livello 5 per i protocolli ordinari e il livello 9 per i protocolli riservati";

- "è emerso che, fra i 29 utenti potenzialmente abilitati alla visione del protocollo oggetto della segnalazione, 21 utenti possedevano profilo e abilitazioni a registri, sezioni e corrispondenti (con relative visibilità) correttamente configurati per ragioni di servizio […] mentre a 7 utenti […] è stato erroneamente associato un profilo riservato agli operatori dell'ufficio protocollo";

- "a seguito della segnalazione pervenuta, la situazione è stata tempestivamente verificata e le configurazioni errate sono state prontamente corrette";

- "per evitare il protrarsi di tale ipotetica erronea configurazione anche ad altri utenti si è operato in modo radicale con l'azzeramento di tutti i profili e successiva riconfigurazione";

- "il profilo [relativo al RPD dell'Ente] non è utilizzato e non risulta attivo";

- "per quanto riguarda la durata della presunta violazione si presume che essa possa avere eventualmente avuto luogo tra la data di protocollazione della nota in argomento, ovvero il XX e la mattina del 28/03/2025";

- "[nel] momento in cui si è verificata la presunta violazione dei dati personali in argomento ha riguardato un periodo di transizione in cui l'intero apparato dell'Ente ex Provincia di Sassari era impegnato nella complessa e articolata attività di divisione con avvio dei due nuovi Enti (Città metropolitana di Sassari e la Provincia nord est Gallura) che ha riguardato la successione anche nelle infrastrutture tecniche e informatiche".

3. Esito dell'attività istruttoria.

Nella cornice del Regolamento e del Codice, il datore di lavoro può trattare i dati personali dei lavoratori se il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento oppure per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (v. artt. 6, par. 1, lett. c) ed e), e parr. 2 e 3, e 88 del Regolamento, nonché 2-ter del Codice).

Il trattamento di dati appartenenti a categorie particolari (v. art. 9 del Regolamento), in ambito lavorativo, può essere legittimamente posto in essere solo quando sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. b), del Regolamento; v. pure, art. 88, e cons. 51-53 del Regolamento; cfr. "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, del d.lgs 10 agosto 2018, n. 101", doc. web n. 9124510), nonché, in taluni casi, al ricorrere di "motivi di interesse pubblico rilevante" (art. 9, par. 2, lett. g) del Regolamento e art. 2-sexies, spec. lett. dd), del Codice).

Con specifico riguardo al trattamento dei dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza, si evidenzia che esso può avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda

garanzie appropriate per i diritti e le libertà degli interessati (art. 10 del Regolamento), ossia solo qualora il trattamento sia autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-octies, del Codice).

La normativa europea prevede che "gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del […] regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto […]" (art. 6, par. 2, del Regolamento). Al riguardo, si evidenzia che l'operazione di "comunicazione" di dati personali a terzi, da parte di soggetti pubblici, è ammessa solo al ricorre delle condizioni previste, in particolare, dall'art. 2-ter, commi 1, 1-bis, 2 e 4, par. 1, lett. a), del Codice; ciò fermo restando che, qualora oggetto di comunicazione siano anche dati personali appartenenti a categorie particolari o relativi a condanne penali e reati, devono essere rispettate le ulteriori condizioni e garanzie previste dagli artt. 9 e 10 del Regolamento, nonché 2-sexies e 2-octies del Codice.

Il titolare del trattamento è tenuto, in ogni caso, a rispettare i principi in materia di protezione dei dati, fra i quali quello di "liceità, correttezza e trasparenza", "minimizzazione dei dati" e "integrità e riservatezza", in base ai quali i dati personali devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato", "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" e "trattati in maniera da garantire un'adeguata sicurezza […], compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (art. 5, par. 1, lett. a), c) ed f), del Regolamento).

Inoltre, in base al principio di "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" (art. 25 del Regolamento), il titolare del trattamento "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento [deve] mette[re] in atto misure tecniche e organizzative adeguate […] volte ad attuare in modo efficace i principi di protezione dei dati […] e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del […] regolamento e tutelare i diritti degli interessati"; devono, inoltre, essere messe "in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per […] l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica" (cfr. le "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020, ove, in particolare, si evidenzia che "il titolare dovrebbe prevedere limitazioni quanto ai soggetti abilitati all'accesso e alla tipologia dell'accesso ai dati personali sulla base di una valutazione della necessità e assicurare che i dati personali siano realmente accessibili a chi ne ha bisogno in caso di necessità", par. 55).

Il titolare del trattamento, secondo il paradigma della "responsabilizzazione", che informa la disciplina eurounitaria in materia di protezione dei dati, "è competente per il rispetto [dei principi di protezione dei dati] e [deve essere] in grado di comprovarlo" (art. 5, par. 2, del Regolamento; v. anche art. 24 dello stesso).

Come da tempo chiarito dal Garante con provvedimenti a carattere generale e decisioni su singoli casi, le amministrazioni, anche quando operano come datrici di lavoro, devono adottare le misure più opportune per prevenire la conoscibilità ingiustificata di dati personali da parte di terzi o soggetti diversi dal destinatario (cfr. punto 5.3 delle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", provv. del 14 giugno 2007, pubblicate in G.U. 13 luglio 2007, n. 161 e in www.gpdp, doc. web n. 1417809). I dati personali dei dipendenti, trattati per finalità di gestione del rapporto di lavoro, non possono,

infatti, di regola, essere messi a conoscenza di soggetti diversi da coloro che sono parte dello specifico rapporto di lavoro (cfr. definizioni di “dato personale” e “interessato”, contenuta nell’art. 4, par. 1, n. 1, del Regolamento), ovvero di coloro che - anche tenuto conto della definizione di “terzo”, contenuta nell’art. 4, par. 1, n. 10, del Regolamento - non siano legittimati a trattarli in ragione delle mansioni assegnate e delle scelte organizzative del titolare del trattamento. Diversamente, nessuna violazione della disciplina di protezione dei dati personali può essere riscontrata nelle ipotesi in cui i soggetti, cui fanno capo specifiche mansioni, vengano a conoscenza di dati personali degli interessati, quando sia necessario per lo svolgimento delle funzioni loro attribuite.

In tale quadro, il Garante ha in più occasioni dichiarato l’illecita conoscibilità dei dati personali di alcuni dipendenti da parte di loro colleghi, in ragione della scorretta configurazione dei sistemi di gestione documentale (provv.ti 24 marzo 2022, doc. web n. 9763051, n. 98; 11 febbraio 2021, n. 50, doc. web n. 9562866; 29 ottobre 2020, n. 204, doc. web n. 9513059; 11 ottobre 2012, n. 280, doc. web n. 2097560; 12 giugno 2014, n. 298, doc. web n. 3318492).

Anche nell’ambito dei trattamenti di dati personali effettuati mediante i sistemi di gestione documentale è, infatti, necessario adottare misure tecniche e organizzative per assicurare l’accesso selettivo alla documentazione presente nel protocollo informatico, al fine di evitare la consultabilità di documenti da parte di personale non autorizzato, ricorrendo in particolare a procedure differenziate e/o riservate con riguardo alla protocollazione di documenti contenenti dati personali dei dipendenti e inerenti lo specifico rapporto di lavoro.

All’esito dell’istruttoria relativa alla notifica di violazione di dati personali e al connesso citato reclamo, risulta accertato che la Città Metropolitana, subentrata alla Provincia di Sassari nei rapporti successori, ha configurato in maniera non corretta il proprio protocollo informatico, rendendo accessibili documenti contenenti dati personali, tra cui quelli della reclamante, a soggetti che, in ragione del ruolo ricoperto e delle mansioni svolte, non potevano considerarsi autorizzati al trattamento di tali dati.

Per quanto concerne la specifica nota oggetto di reclamo, dall’istruttoria e dall’esame delle dichiarazioni rese in sede di memoria difensiva, anche ai sensi dell’art. 168 del Codice, è emerso che la stessa, per effetto della scorretta configurazione del protocollo informatico, era visualizzabile da ventinove persone fisiche operanti all’interno dell’Ente. A sette di queste era stato, tuttavia, erroneamente attribuito il profilo di autorizzazione riservato ai soli operatori dell’ufficio di protocollo. Resta, pertanto, accertato che, fino al 29 marzo 2025, la Città Metropolitana ha omesso di configurare il protocollo informatico in maniera coerente con l’effettivo profilo di autorizzazione di talune persone fisiche operanti all’interno della propria struttura organizzativa.

La Città Metropolitana ha, pertanto, omesso di dare attuazione ai principi di protezione dei dati, con particolare riguardo a quelli di “minimizzazione”, “integrità e riservatezza”, “responsabilizzazione” e “protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”, in violazione degli artt. 5, par. 1, lett. c) ed f), e par. 2, nonché 25, del Regolamento.

La mancata adozione misure tecniche e organizzative adeguate a garantire la necessaria riservatezza dei documenti acquisiti al protocollo informatico - dove transitano tutte le documentazioni afferenti alla gestione e all’attività istituzionale dell’Ente - ha, altresì, dato luogo, anche con riguardo ai dati personali della reclamante nella vicenda oggetto di reclamo, a comunicazioni di dati personali a soggetti che devono considerarsi terzi, in quanto non autorizzati al trattamento. Ciò con conseguente violazione degli artt. 5, par. 1, lett. a) e 6, par. 1, lett. c) ed e), e parr. 2 e 3, del Regolamento e 2-ter del Codice, nonché, in relazione ai dati personali appartenenti a categorie particolari o relativi a reati, degli artt. 9 e 10 del Regolamento e 2-sexies e 2-octies del Codice.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice , seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dalla Città Metropolitana di Sassari, per aver trattato dati personali della reclamante e di altri interessati, in ragione della scorretta configurazione del proprio protocollo informatico, in violazione degli artt. 5, par. 1, lett. a) e f), e par. 2, 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, 10 e 25 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice.

Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, le violazioni più gravi, relative agli artt. 5, par. 1, lett. a) e f), e par. 2, 6, par. 1, lett. c) ed e), 9 e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice, sono soggette alla sanzione prevista dall'art. 83, par. 5, del Regolamento, come richiamato anche dall'art. 166, comma 2, del Codice, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti - atteso che il titolare del trattamento ha dichiarato di aver proceduto all'"azzeramento di tutti i profili e successiva riconfigurazione" - non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del Regolamento.

5. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Tenuto conto che:

- la violazione è stata posta in essere nonostante il Garante, fin dal 2007, abbia fornito ai datori di lavoro pubblici e privati indicazioni (v. in particolare, par. 5 delle citate Linee guida del 14 giugno 2007, n. 161) sul corretto trattamento dei dati nell'ambito della gestione del

rapporto di lavoro (cfr. art. 83, par. 2, lett. a), del Regolamento);

- la violazione ha riguardato tutti i dati personali transitati sul protocollo informatico, inclusi quelli della reclamante, atteso che la scorretta configurazione del protocollo informatico riguardava la struttura organizzativa dell'Ente nel suo complesso, protrattasi fino all'avvenuta riconfigurazione dell'intero sistema, che ha avuto luogo nel corso dell'istruttoria, come emerge dagli atti (cfr. art. 83, par. 2, lett. a), del Regolamento);

- per quanto riguarda la specifica nota oggetto di reclamo, il trattamento ha riguardato dati personali delicati, in quanto afferenti a una segnalazione di una presunta condotta ritenuta astrattamente rilevante ai fini disciplinari, ancorché, come dichiarato dall'Ente, la visibilità di detta nota agli utenti non autorizzati ha avuto luogo in un intervallo temporale limitato, vale a dire tra il 25 marzo 2025 e la mattina del 28 marzo 2025 (cfr. art. 83, par. 2, lett. a) e g), del Regolamento);

- la violazione ha carattere colposo, essendo stata causata da un errore di configurazione del protocollo informatico (cfr. art. 83, par. 2, lett. b), del Regolamento);

- il trattamento ha riguardato anche dati particolari appartenenti alle categorie particolari di cui all'art. 9 del Regolamento, nonché dati relativi a reati di cui all'art. 10 del Regolamento (cfr. art. 83, par. 2, lett. g), del Regolamento),

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia medio (cfr. Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR" del 24 maggio 2023, punto 60).

Ciò premesso, nel considerare che il titolare del trattamento è un soggetto pubblico di rilevanza provinciale (circa 310.000 abitanti), si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

- la Città Metropolitana ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria (cfr. art. 83, par. 2, lett. f), del Regolamento);

- non risultano precedenti violazioni pertinenti commesse dalla Città Metropolitana (cfr. art. 83, par. 2, lett. e), del Regolamento);

- quantomeno nel periodo in cui hanno avuto luogo gli specifici fatti oggetto di reclamo, era in corso la migrazione delle attività, anche a livello informatico, dalla Provincia di Sassari alla Città Metropolitana di Sassari (cfr. art. 83, par. 2, lett. k), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 12.000 (dodicimila) per la violazione degli artt. 5, par. 1, lett. a) e f), e par. 2, 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, 10 e 25 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione della natura delicata dei dati oggetto di trattamento, che, nel caso della reclamante, afferivano a una segnalazione di una presunta condotta ritenuta astrattamente rilevante ai fini disciplinari e, pertanto, a un'informazione che, se conosciuta da soggetti non autorizzati, può esporre l'interessata a un pregiudizio, anche reputazionale, sul piano personale e professionale, indipendentemente dal fatto che alla segnalazione sia seguita o meno l'apertura di un

procedimento disciplinare.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dalla Città Metropolitana di Sassari per la violazione degli artt. 5, par. 1, lett. a) e f), e par. 2, 6, par. 1, lett. c) ed e), e parr. 2 e 3, 9, 10 e 25 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice, nei termini di cui in motivazione;

ORDINA

alla Città Metropolitana di Sassari, in persona del legale rappresentante pro-tempore, con sede legale in Piazza d'Italia, 31 - 07100 Sassari (SS), C.F. 92182020906, di pagare la somma di euro 12.000 (dodicimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

alla predetta Città Metropolitana, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 12.000 (dodicimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

- ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità;

- ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 11 giugno 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Montuori