

PARERI E PROVVEDIMENTI SANZIONATORI DEL GARANTE DELLA PRIVACY AFFERENTI LE ATTIVITÀ DEGLI ENTI LOCALI

In questa miscellanea di pareri e provvedimenti sanzionatori adottati dal Garante della Privacy sono riportati, oltre ai dati identificativi dei predetti documenti, gli elementi salienti utili per comprendere le fattispecie di violazioni alle disposizioni in materia di trattamento dei dati personali di cui al Regolamento UE 2016/679 e al d.lgs. n. 196/2003 esaminate e le motivazioni che hanno determinato la comminazione delle rispettive sanzioni.

Sono riportati anche gli estremi di alcuni provvedimenti del Garante di carattere generale nonché ordinanze-ingiunzioni dirette a sanzionare soggetti giuridici diversi dagli enti locali, ma le cui fattispecie potrebbero ricorrere nello svolgimento di attività di questi ultimi.

INDICE PER ARGOMENTI

Abusi edilizi - Accesso civico - Accesso documentale - Albo pretorio - Archivio online -
Atti giudiziari - Busta paga - Concorso per assunzioni - Contratti pubblici - Contributi Sovvenzioni
Curriculum vitae - Dati sensibili - Dati giudiziari - Data breach - Debiti fuori bilancio - Defunti -
Deliberazioni - Diritti interessato - Diritto di accesso ai dati - Elettorale - Incarichi professionali -
Informativa - Notificazione atti - Ordinanze sindacali - Personale - Polizia Locale - Plurindirizzi -
Procedimento disciplinare - Programmi per accesso utenti a servizi - Protocollo - Pubblicazioni facoltative
Rapporto di lavoro - Rappresentanti di persone giuridiche - Registro accessi - Responsabile Protezione Dati
Rifiuti raccolta differenziata - Servizi esternalizzati - Strumenti e programmi informatici - Trattamento
Sanitario Obbligatorio - Varie - Video-sorveglianza - Zona a Traffico Limitato

ABUSI EDILIZI

Provvedimento Garante : n. 384 del 21/09/2017
Fattispecie : pubblicazione nell'Albo pretorio online di un' ordinanza di demolizione opere abusive e ripristino dello stato dei luoghi , contenente dati personali e fiscali e dell'immobile; reperibile dopo oltre due anni nell'archivio dell'Albo pretorio e su motori di ricerca
Violazioni : assenza di un fondamento giuridico per la diffusione di dati personali; violazione del principio di pertinenza e non eccedenza dei dati trattati
Sanzione: euro 500,00

Parere Garante: n. 449 del 07/08/2018
Fattispecie: parere su richiesta di riesame dell'istanza di accesso civico, denegata, volta a ottenere: 1. «l' accesso ai dati relativi agli immobili e alle opere realizzati abusivamente, relativi all'Elenco dei rapporti degli ufficiali ed agenti di Polizia Giudiziaria riguardante opere o lottizzazioni abusive , pubblicato [in data identificata

in atti] all'Albo Pretorio del Comune di»;

2. **l'accesso ai due rapporti**, identificati in atti con data e numero di protocollo, citati nel predetto elenco di cui supra al n. 1;
3. **«l'accesso alla documentazione che la pubblica amministrazione ha prodotto nell'esercizio delle sue istituzionali funzioni amministrative**, in merito alle opere abusive relative ai rapporti [di cui supra al n. 2]»;
4. **«l'accesso alla seguente informazione: indicazione di quali organi preposti al controllo erano presenti durante i sopraccitati sopralluoghi»;**
5. **«l'accesso alla seguente informazione: quantificazione ipotizzata delle mancate entrate tributarie a favore dell'Ente comunale a causa delle opere o lottizzazioni abusive sopraccitate, a partire dal momento della realizzazione dell'illecito»;**
6. **«l'accesso alla seguente informazione: quantificazione dei danni di natura idrogeologica stimati per via della realizzazione delle opere o lottizzazioni abusive sopraccitate».**

Dagli atti risulta che i controinteressati hanno presentato opposizione all'accesso civico, rappresentando, fra l'altro, di avere richiesto una proroga al termine indicato nell'ordinanza di demolizione e di rimessa in pristino dello stato dei luoghi, concessa dal Comune, anche al fine (come risulta in una delle opposizioni) di conformare i lavori svolti alla vigente disciplina urbanistica. L'opposizione era, altresì, motivata dalla necessità di evitare il grave pregiudizio all'attività economica esercitata, a causa della divulgazione degli atti del procedimento anche considerando l'avvio del procedimento penale a carico dei presunti autori degli abusi.

Il Comune ha negato l'accesso civico, rappresentando, fra l'altro, l'esistenza di un pregiudizio con riferimento alla tutela di interessi economici e commerciali di una persona fisica e giuridica, nonché alla protezione dei dati personali dei controinteressati (art. 5-bis, comma 2, lett. a) e c), del d. lgs. n. 33/2013).

In relazione al regime di pubblicità delle informazioni riguardanti opere abusive, si ricorda che la specifica normativa statale di settore prevede espressamente che **«il segretario comunale redige e pubblica mensilmente, mediante affissione nell'albo comunale, i dati relativi agli immobili e alle opere realizzati abusivamente, oggetto dei rapporti degli ufficiali ed agenti di polizia giudiziaria e delle relative ordinanze di sospensione»** (art. 31, comma 7, del d.P.R. n. 380 del 6/6/2001).

Dagli atti risulta che il Comune ha provveduto alla predetta pubblicazione sull'albo pretorio online in data 2/2/2018, oscurando i dati personali dei committenti. Tale documento risulta già in possesso dell'istante.

Contenuto parere: Il Garante non concorda con quanto affermato dall'istante, nella richiesta di accesso civico, laddove viene richiamata l'applicazione dell'art. 6, comma 1, del d. lgs. n. 33/2013 per ottenere l'ostensione integrale della documentazione richiesta. Ciò in quanto, fermo restando il rispetto della «qualità delle informazioni» oggetto di pubblicazione obbligatoria, richiamata nella predetta disposizione, **i principi e la disciplina di protezione dei dati personali** – come peraltro previsto anche dagli artt. 1, comma 2, e 7-bis del d. lgs. n. 33/2013 (v. altresì art. 8, comma 3) – **devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza.**

Infatti, come già affermato dal Garante, **«Laddove l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento nel proprio sito web istituzionale è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni.**

I soggetti pubblici, infatti, in conformità ai principi di protezione dei dati, **sono tenuti a ridurre al minimo l'utilizzazione di dati personali e di dati identificativi ed evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità (cd. "principio di necessità"** di cui all'art. 3, comma 1, del Codice). Pertanto, anche in presenza degli obblighi di pubblicazione di atti o documenti contenuti nel d. lgs. n. 33/2013, i soggetti chiamati a darvi attuazione **non possono comunque "rendere [...] intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione"** (art. 4, comma 4, del d. lgs. n. 33/2013).

È, quindi, **consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principio di pertinenza e non eccedenza"** di cui all'art. 11, comma 1, lett. d, del Codice). Di conseguenza, **i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti»** (provv. n. 243 del 15/5/2014).

Quanto alla **possibilità di conoscere, tramite l'istituto dell'accesso civico, i dati personali non oggetto di pubblicazione da parte del Comune (fra cui i dati relativi identificativi degli autori dei presunti abusi) o i verbali di sopralluogo effettuati dalla polizia municipale, deve essere tenuta in considerazione la circostanza per la quale** – a differenza dei documenti a cui si è avuto accesso ai sensi della l. n. 241 del 7/8/1990 – **i dati e i documenti che si ricevono a seguito di una istanza di accesso civico divengono «pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7»,** sebbene il loro ulteriore trattamento

vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, del d. lgs. n. 33/2013).

Di conseguenza, è **anche alla luce di tale amplificato regime di pubblicità dell'accesso civico che va valutata l'esistenza di un possibile pregiudizio concreto alla protezione dei dati personali dei soggetti controinteressati**, in base al quale decidere se rifiutare o meno l'accesso ai documenti richiesti.

Il Garante afferma che Comune abbia correttamente respinto l'accesso civico alla documentazione richiesta.

Ciò in quanto, tenendo conto della tipologia e della natura dei dati e delle informazioni personali contenuti nella documentazione oggetto dell'istanza di accesso civico, nel caso in esame, la generale conoscenza dei dati e delle informazioni richieste potrebbe determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei soggetti controinteressati, con possibili ripercussioni negative sul piano lavorativo, professionale, personale e sociale (cfr. par. 8.1 delle Linee guida dell'ANAC in materia di accesso civico, cit.). L'ostensione richiesta, unita peraltro al particolare regime di pubblicità dei dati oggetto di accesso civico e al ristretto ambito territoriale del Comune interessato di soli 4000 abitanti, può arrecare ai soggetti controinteressati, a seconda delle ipotesi e del contesto in cui le informazioni fornite possono essere utilizzate da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Provvedimento Garante : n. 139 del 09/07/2020

Fattispecie : sul sito web istituzionale del Comune di ..., nella sezione Servizi online/Albo pretorio storico, erano visibili e liberamente scaricabili **i documenti del settore urbanistica-edilizia** che contenevano dati e informazioni personali dei soggetti interessati, quali i dati anagrafici e di residenza, i dati identificativi e catastali dell'immobile di proprietà, le informazioni inerenti alla realizzazione di opere abusive e le risultanze dal verbale di sopralluogo, i rilievi fotografici della veranda del proprio appartamento, etc..

Violazioni: la diffusione dei dati personali dei reclamanti risulta illecita in quanto:

- a) non risultavano necessari rispetto alla finalità del trattamento, con particolare riferimento all'avvenuta diffusione della data e luogo di nascita, della residenza, dei dati identificativi e catastali dell'immobile di proprietà, delle informazioni inerenti alla realizzazione di opere abusive, in violazione del principio di minimizzazione e, dunque, dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. c), del RGPD;
- b) si è protratta per più di quindici giorni previsti dall'art. 124, comma 1, del d. lgs. n. 267/2000 per la pubblicazione nell'albo pretorio, in assenza quindi – per il periodo temporale eccedente – di idonei presupposti normativi per la diffusione di dati personali e, dunque, in violazione dell'art. 19 comma 3 del Codice (vigente all'epoca dei fatti e il cui contenuto è ora riprodotto nell'art. 2-ter, commi 1 e 3, del Codice), nonché dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a e c; 6, par. 1, lett. c ed e, par. 2 e par. 3, lett. b, del RGPD.

Sanzione: euro 2.000,00

Provvedimento Garante : n. 91 dell'11/03/2021

Fattispecie : pubblicazione nel sito web istituzionale del Comune, visionabili e scaricabili attraverso i motori di ricerca, di due **ordinanze sindacali per la rimozione o demolizione di opere abusive** e con ordine di sgombero immediato, pubblicate nel link del sito web istituzionale dedicato alle ordinanze del Sindaco, in cui erano riportati dati e informazioni personali del reclamante e dei suoi familiari (con indicazione della data e del luogo di nascita, del codice fiscale, della residenza), con cui è stato ordinato lo sgombero immediato di immobili e l'ingiunzione di pagamento pari a € 20.000 a titolo di sanzione amministrativa, nell'ambito di una vicenda riferita a un procedimento aperto per opere eseguite in assenza del permesso di costruire.

Violazioni : e si rileva l'illiceità del trattamento di dati personali effettuato dal Comune, in quanto la diffusione dei dati e delle informazioni personali del reclamante e dei suoi familiari, contenuti nelle due ordinanze sindacali pubblicate online risulta:

- a) non conforme al principio di «minimizzazione» dei dati – con riferimento all'indicazione in chiaro della data e del luogo di nascita, del codice fiscale e della residenza – considerando che gli stessi non risultano essere stati «limitati a quanto necessario rispetto alle finalità per le quali sono trattati», in violazione dell'art. 5, par. 1, lett. c), del RGPD;
- b) priva di idonei presupposti normativi per il periodo eccedente i quindici giorni previsti dall'art. 124, comma 1, del d. lgs. n. 267/2000 per la pubblicazione nell'albo pretorio, in violazione dell'art. 2-ter, commi 1 e 3, del Codice; nonché dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD

Sanzione: euro 3.000,00

Provvedimento Garante : n. 254 del 24/06/2021

Fattispecie : pubblicazione on line, tramite piattaforma Internet fornita da una società esterna, di un'ordinanza con cui è stata ordinata la demolizione di una struttura in acciaio realizzata abusivamente, che fungeva da copertura del sottostante fabbricato per il quale era stato invece rilasciato permesso di costruire in sanatoria; la diffusione illecita riguarda dati e informazioni personali del reclamante (fra cui nome e cognome, data e luogo di nascita, domicilio, dati catastali dell'immobile di proprietà, informazioni sul procedimento per abuso edilizio nei suoi confronti).

Violazioni : il Comune non ha adempiuto all'obbligo di adottare, fin dall'inizio del trattamento - "by design" - (art. 25, par. 1, RGDP) :

- idonee misure tecniche e organizzative volte a minimizzare i dati pubblicati online, evitando la diffusione di dati non «limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Ciò con particolare riferimento all'avvenuta diffusione della data e luogo di nascita, nonché del domicilio del reclamante.
- gli opportuni «accorgimenti per la tutela dei dati personali, provvedendo a oscurare nella documentazione pubblicata i dati e le informazioni idonei a identificare, anche in maniera indiretta, i soggetti interessati» dopo la scadenza dei 15 giorni prevista per la pubblicazione nell'albo pretorio (come indicato nelle Linee guida del Garante n. 243 del 2014)
- Quanto alla circostanza evidenziata nelle memorie difensive, per la quale l'«atto è stato pubblicato ai sensi del DPR 380/01» e i dati pubblicati sarebbero pertinenti e non eccedenti in quanto l'ordinanza sarebbe stata «di rilevante interesse pubblico», occorre evidenziare che il Comune si è limitato a rinviare genericamente al predetto d.p.r. senza individuare alcuna disposizione che preveda nel concreto un obbligo di pubblicazione dell'ordinanza oggetto di reclamo, che allo stato infatti non risulta ivi contenuto. Il d.p.r. citato, pertanto, non può costituire, alla luce di quanto rappresentato, un'idonea base normativa per diffondere i dati personali del soggetto interessato ai sensi dell'art. 2-ter, commi 1 e 3, del Codice.
- diffusione di dati (data e luogo di nascita, domicilio, dati catastali dell'immobile, informazioni sul procedimento per abuso edilizio) "non limitati alla finalità del trattamento" in violazione del principio di "minimizzazione" dei dati ex art. 5, prf. 1, lett. c), del RGDP; assenza di presupposto normativo per la pubblicazione oltre i 15 giorni prescritti dall'art. 124, c.1, d.lgs. 267/2000.

Sanzione: euro 1.000,00

ACCESSO CIVICO**Parere Garante: n. 360 del 10/08/2017**

Fattispecie: parere previsto dall'art. 5, comma 7, del d. lgs. n. 33/2013, nell'ambito del procedimento relativo a una richiesta di riesame sul provvedimento di diniego di un'istanza di accesso civico generalizzato avente ad oggetto: dapprima, la «copia in forma riassuntiva contenente i dati del committente, descrizione dell'intervento, località del cantiere, tecnico progettista, delle **Segnalazioni Certificate di Inizio Attività (SCIA) e delle Comunicazioni Inizio Attività Asseverata (CILA) concernenti l'attività degli interventi edili** da attuarsi nel territorio comunale, presentate dal 01/01/2017 al 25/02/2017»; e, successivamente, nel corso del procedimento, di ricevere la copia integrale di tutte le Segnalazioni Certificate di Inizio Attività (SCIA) e di tutte le Comunicazioni Inizio Attività Asseverata (CILA), presentate al Comune nei mesi di gennaio e febbraio 2017.

Contenuto del parere. Il Garante ritiene che correttamente il Comune ha respinto l'istanza di accesso civico sia integrale che parziale, per le ragioni di seguito esposte.

Regime di pubblicità della SCIA e della CILA : dopo l'abrogazione (ad opera del d. lgs. n. 97/2016) dell'art. 23, comma 1, lett. a), del d. lgs. n. 33/2013, che prevedeva l'obbligo da parte delle pp.aa. di pubblicare sul sito web istituzionale gli «elenchi dei provvedimenti» adottati «con particolare riferimento ai provvedimenti finali dei procedimenti di: a) autorizzazione o concessione», ai quali, secondo l'orientamento adottato dall'ANAC dovevano ritenersi equiparati anche la DIA e la SCIA (Orientamento n. 11 del 21/5/2014, **non esiste un obbligo di pubblicazione da parte delle pp.aa. delle Segnalazioni certificate di inizio di attività-SCIA o delle Comunicazioni di inizio lavori asseverata-CILA presentate all'ente, né in forma integrale né in forma riassuntiva.**

Per quanto concerne la disposizione contenuta nell'**art. 20, comma 6, del d.P.R. n. 380/2001 che prevede la pubblicazione sull'albo pretorio della mera «notizia» dell'«avvenuto rilascio del permesso di costruire»** (i cui estremi sono peraltro «indicati nel cartello esposto presso il cantiere, secondo le modalità stabilite dal regolamento edilizio») e **non del provvedimento integrale**, si tratta di una norma di settore attinente al solo «procedimento per il rilascio del permesso di costruire» che non è ripetuta (né richiamata) per i procedimenti relativi agli altri titoli edilizi, come la CILA o la SCIA – disciplinati nel medesimo testo unico in materia edilizia – ai quali, di conseguenza, non è applicabile lo stesso regime di pubblicità previsto per la notizia dell'avvenuto rilascio del permesso di costruire.

Sull'esistenza e sulla valutazione di un pregiudizio concreto in materia di protezione dei dati personali :

Come sostenuto dall'ANAC, con riferimento ai provvedimenti finali di autorizzazione e concessione, stante l'abrogazione dell'art. 23, comma 1, lett. a), del d. lgs. n. 33/2013, «Resta ferma la possibilità di esercitare il diritto di accesso civico generalizzato», ma nel rispetto «degli artt. 5, co. 2 e 5-bis del d.lgs. 33/2013».

Ciò vuol dire che non è possibile derogare alle disposizioni che, in caso di accesso civico, sanciscono **il necessario**

coinvolgimento dei soggetti controinteressati, né a quelle che prevedono il rifiuto dell'accesso civico nel caso della sussistenza di un pregiudizio concreto alla protezione dei dati personali.

Quanto alla richiesta di accesso civico alle SCIA e alle CILA presentate al Comune nei mesi di gennaio e febbraio 2017, si rinvia in primo luogo al contenuto delle **Linee guida dell'ANAC** in materia di accesso civico, laddove è precisato in particolare (par. 8.1) che:

«La disciplina in materia di protezione dei dati personali prevede che **ogni trattamento** – quindi anche una comunicazione di dati personali a un terzo tramite l'accesso generalizzato – **deve essere effettuato "nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale [...]"**, ivi inclusi il diritto alla reputazione, all'immagine, al nome, all'oblio, nonché i diritti inviolabili della persona di cui agli artt. 2 e 3 della Costituzione. Nel quadro descritto, **anche le comunicazioni di dati personali nell'ambito del procedimento di accesso generalizzato non devono determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà delle persone cui si riferiscono tali dati** ai sensi dell'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea e della giurisprudenza europea in materia»;

«Ai fini della **valutazione del pregiudizio concreto**, vanno prese in considerazione le conseguenze – anche legate alla sferamorale, relazionale e sociale – che potrebbero derivare all'interessato (o ad altre persone alle quali esso è legato da un vincolo affettivo) dalla conoscibilità, da parte di chiunque, del dato o del documento richiesto, tenuto conto delle implicazioni derivanti dalla previsione di cui all'art. 3, comma 1, del d. lgs. n. 33/2013, in base alla quale i dati e i documenti forniti al richiedente tramite l'accesso generalizzato sono considerati come «pubblici», sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 7 del d. lgs. n. 33/2013). Tali conseguenze potrebbero riguardare, ad esempio, future azioni da parte di terzi nei confronti dell'interessato, o situazioni che potrebbero determinare l'estromissione o la discriminazione dello stesso individuo, oppure altri svantaggi personali e/o sociali. In questo quadro, può essere valutata, ad esempio, l'eventualità che l'interessato possa essere esposto a minacce, intimidazioni, ritorsioni o turbative al regolare svolgimento delle funzioni pubbliche o delle attività di pubblico interesse esercitate, che potrebbero derivare, a seconda delle particolari circostanze del caso, dalla conoscibilità di determinati dati. Analogamente, vanno tenuti in debito conto i casi in cui la conoscibilità di determinati dati personali da parte di chiunque possa favorire il verificarsi di eventuali furti di identità o di creazione di identità fittizie attraverso le quali esercitare attività fraudolente»;

«Nel valutare l'impatto nei riguardi dell'interessato, vanno tenute in debito conto anche le ragionevoli aspettative di quest'ultimo riguardo al trattamento dei propri dati personali al momento in cui questi sono stati raccolti, ad esempio nel caso in cui le predette conseguenze non erano prevedibili al momento della raccolta dei dati. Per verificare l'impatto sfavorevole che potrebbe derivare all'interessato dalla conoscibilità da parte di chiunque delle informazioni richieste, l'ente destinatario della richiesta di accesso generalizzato deve far riferimento a diversi parametri, tra i quali, anche la natura dei dati personali oggetto della richiesta di accesso o contenuti nei documenti ai quali si chiede di accedere, nonché il ruolo ricoperto nella vita pubblica, la funzione pubblica esercitata o l'attività di pubblico interesse svolta dalla persona cui si riferiscono i predetti dati» ;

«va considerato altresì che la **sussistenza di un pregiudizio concreto alla protezione dei dati personali può verificarsi con più probabilità per talune particolari informazioni** – come ad esempio situazioni personali, familiari, professionali, patrimoniali – di persone fisiche destinatarie dell'attività amministrativa o intervenute a vario titolo nella stessa e che, quindi, non ricoprono necessariamente un ruolo nella vita pubblica o non esercitano funzioni pubbliche o attività di pubblico interesse. Ciò anche pensando, come già visto, alle ragionevoli aspettative di confidenzialità degli interessati riguardo a talune informazioni in possesso dei soggetti destinatari delle istanze di accesso generalizzato o la non prevedibilità delle conseguenze derivanti a questi ultimi dalla conoscibilità da parte di chiunque di tali dati».

Si richiama inoltre l'attenzione sulla circostanza che – a differenza dei documenti a cui si è avuto accesso ai sensi della l. n. 241/1990 – **i dati e i documenti ricevuti a seguito di una istanza di accesso civico sono soggetti a un particolare regime di pubblicità, essendo previsto che «Tutti i documenti, le informazioni e i dati oggetto di accesso civico [...] sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7»**, sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, del d. lgs. n. 33/2013).

In tale contesto, con particolare riferimento al caso sottoposto all'attenzione del Garante, si ritiene che, con riferimento all'accesso civico a tutte le Segnalazioni Certificate di Inizio Attività (SCIA) e a tutte le Comunicazioni Inizio Attività Asseverata (CILA) presentate all'ente dall'1/1/2017 al 25/02/2017, **l'amministrazione abbia correttamente respinto l'istanza**. Ciò, sia nel caso in cui la domanda di accesso civico abbia come oggetto la copia integrale dei documenti (come chiesto nell'istanza di riesame), sia nel caso in cui l'oggetto dell'accesso sia limitato (come richiesto nella domanda iniziale) alla ricezione di «copia in forma riassuntiva» dei dati del committente e del tecnico progettista, corredati dalla descrizione dell'intervento e della località del cantiere

(inteso come accesso civico parziale ai sensi dell'art. 5-bis, comma 4, d. lgs. n. 33/2013).

Infatti, ai sensi della normativa vigente e tenendo anche conto delle richiamate indicazioni contenute nelle Linee guida dell'ANAC, **l'ostensione dei predetti documenti o informazioni, considerando la quantità e qualità dei dati personali coinvolti, uniti al particolare regime di pubblicità dei dati e documenti oggetti di accesso civico, è suscettibile di determinare, a seconda delle ipotesi e del contesto in cui possono essere utilizzati da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.**

Per gli stessi motivi, il medesimo pregiudizio concreto alla tutela della protezione dei dati personali, potrebbe realizzarsi anche nel caso di un eventuale e più limitato accesso parziale – come richiesto dall'istante in una nota interlocutoria prima della richiesta di riesame – avente a oggetto i soli dati del tecnico progettista (senza quelli relativi al committente), corredati però dalla descrizione dell'intervento e della località dove avviene il lavoro con via e numero civico. Anche in tale caso si concorda con quanto evidenziato dal Comune laddove si sostiene che «dai dati in questione è possibile risalire all'esistenza del rapporto professionale tra committente e progettista» e che «anche se si oscurassero i dati del committente, l'indicazione dell'immobile oggetto dell'intervento consentirebbe di risalire all'identità del relativo proprietario tramite una visura catastale».

A ciò si aggiunge la circostanza, non dirimente ma comunque sintomatica, che nel caso esaminato, il richiedente l'accesso è una impresa privata, la XX, che, dall'istruttoria effettuata dal Comune, risulta avere effettuato con carattere sistematico analoghe richieste di accesso a diversi enti locali e ha tra le sue attività «prevalente» e «secondaria», rispettivamente, la «Gestione database, attività delle banche dati» e lo «Studio e realizzazione di spazi pubblicitari (banner) da pubblicizzare sui propri siti web, per informare, motivare e servire il mercato. Attività di conduzione di campagne di marketing, social media e web marketing. Servizi di gestione dei programmi di fidelizzazione e affiliazione commerciale».

L'insieme delle considerazioni sopra esposte è, pertanto, idonea a configurare, come sostenuto dal Comune, l'esposizione dei soggetti interessati «a un pregiudizio concreto ed estremamente probabile alla tutela del loro interesse alla protezione dei dati personali, in conformità con la disciplina legislativa in materia».

Inoltre, come indicato anche nelle Linee guida dell'ANAC sull'accesso civico, **l'accesso "generalizzato" è servente rispetto alla conoscenza di dati e documenti detenuti dalla p.a.** «Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico» (art. 5, comma 2, del d. lgs. n. 33/2013) (cfr. par. 8.1).

Di conseguenza, quando l'oggetto della richiesta di accesso riguarda documenti contenenti informazioni relative a persone fisiche (e in quanto tali «dati personali») non necessarie al raggiungimento del predetto scopo, oppure informazioni personali di dettaglio che risultino comunque sproporzionate, eccedenti e non pertinenti, l'ente destinatario della richiesta, nel dare riscontro alla richiesta di accesso generalizzato, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato (ivi).

Nel presente caso, come evidenziato dal Comune, la conoscenza indiscriminata dell'ampio set di informazioni e dati personali contenuti nella documentazione oggetto dell'accesso civico (CILA e SCIA), appare non necessaria o comunque sproporzionata, rispetto allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

Parere Garante: n. 449 del 07/08/2018

Fattispecie: parere su richiesta di riesame dell'istanza di accesso civico, denegata, volta a ottenere:

1. «**l'accesso ai dati relativi agli immobili e alle opere realizzati abusivamente, relativi all'Elenco dei rapporti degli ufficiali ed agenti di Polizia Giudiziaria riguardante opere o lottizzazioni abusive**, pubblicato [in data identificata in atti] all'Albo Pretorio del Comune di»;
2. **l'accesso ai due rapporti**, identificati in atti con data e numero di protocollo, citati nel predetto elenco di cui supra al n. 1;
3. «**l'accesso alla documentazione che la pubblica amministrazione ha prodotto nell'esercizio delle sue istituzionali funzioni amministrative**, in merito alle opere abusive relative ai rapporti [di cui supra al n. 2]»;
4. «l'accesso alla seguente informazione: **quali organi preposti al controllo erano presenti durante i sopralluoghi**»;
5. «l'accesso alla seguente informazione: **quantificazione ipotizzata delle mancate entrate tributarie** a favore dell'Ente comunale a causa delle opere o lottizzazioni abusive sopracitate, a partire dal momento della realizzazione dell'illecito»;
6. «l'accesso alla seguente informazione: **quantificazione dei danni di natura idrogeologica stimati per via della realizzazione delle opere o lottizzazioni abusive** sopracitate».

Dagli atti risulta che i controinteressati hanno presentato opposizione all'accesso civico, rappresentando, fra l'altro, di avere richiesto una proroga al termine indicato nell'ordinanza di demolizione e di rimessa in pristino dello stato dei luoghi, concessa dal Comune, anche al fine (come risulta in una delle opposizioni) di conformare i lavori svolti alla vigente disciplina urbanistica. L'opposizione era, altresì, motivata dalla necessità di evitare il grave pregiudizio

all'attività economica esercitata, a causa della divulgazione degli atti del procedimento anche considerando l'avvio del procedimento penale a carico dei presunti autori degli abusi.

Il Comune ha negato l'accesso civico, rappresentando, fra l'altro, l'esistenza di un pregiudizio con riferimento alla tutela di interessi economici e commerciali di una persona fisica e giuridica, nonché alla protezione dei dati personali dei controinteressati (art. 5-bis, comma 2, lett. a) e c), del d. lgs. n. 33/2013).

In relazione al regime di pubblicità delle informazioni riguardanti opere abusive, si ricorda che la specifica normativa statale di settore prevede espressamente che «**il segretario comunale redige e pubblica mensilmente, mediante affissione nell'albo comunale, i dati relativi agli immobili e alle opere realizzati abusivamente, oggetto dei rapporti degli ufficiali ed agenti di polizia giudiziaria e delle relative ordinanze di sospensione**» (art. 31, comma 7, del d.P.R. n. 380 del 6/6/2001).

Dagli atti risulta che il Comune ha provveduto alla predetta pubblicazione sull'albo pretorio online in data 2/2/2018, oscurando i dati personali dei committenti. Tale documento risulta già in possesso dell'istante.

Contenuto parere: Il Garante non concorda con quanto affermato dall'istante, nella richiesta di accesso civico, laddove viene richiamata l'applicazione dell'art. 6, comma 1, del d. lgs. n. 33/2013 per ottenere l'ostensione integrale della documentazione richiesta. Ciò in quanto, fermo restando il rispetto della «qualità delle informazioni» oggetto di pubblicazione obbligatoria, richiamata nella predetta disposizione, **i principi e la disciplina di protezione dei dati personali** – come peraltro previsto anche dagli artt. 1, comma 2, e 7-bis del d. lgs. n. 33/2013 (v. altresì art. 8, comma 3) – **devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza.**

Infatti, come già affermato dal Garante, «**Laddove l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento nel proprio sito web istituzionale è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni.**

I soggetti pubblici, infatti, in conformità ai principi di protezione dei dati, **sono tenuti a ridurre al minimo l'utilizzazione di dati personali e di dati identificativi ed evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità (cd. "principio di necessità" di cui all'art. 3, comma 1, del Codice).** Pertanto, anche in presenza degli obblighi di pubblicazione di atti o documenti contenuti nel d. lgs. n. 33/2013, i soggetti chiamati a darvi attuazione **non possono comunque "rendere [...] intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione"** (art. 4, comma 4, del d. lgs. n. 33/2013).

È, quindi, **consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principio di pertinenza e non eccedenza" di cui all'art. 11, comma 1, lett. d, del Codice).** Di conseguenza, **i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online.** In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti» (prov. n. 243 del 15/5/2014).

Quanto alla **possibilità di conoscere, tramite l'istituto dell'accesso civico, i dati personali non oggetto di pubblicazione da parte del Comune (fra cui i dati relativi identificativi degli autori dei presunti abusi) o i verbali di sopralluogo effettuati dalla polizia municipale, deve essere tenuta in considerazione la circostanza per la quale** – a differenza dei documenti a cui si è avuto accesso ai sensi della l. n. 241 del 7/8/1990 – **i dati e i documenti che si ricevono a seguito di una istanza di accesso civico divengono «pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7»**, sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, del d. lgs. n. 33/2013).

Di conseguenza, è **anche alla luce di tale amplificato regime di pubblicità dell'accesso civico che va valutata l'esistenza di un possibile pregiudizio concreto alla protezione dei dati personali dei soggetti controinteressati**, in base al quale decidere se rifiutare o meno l'accesso ai documenti richiesti.

Il Garante afferma che Comune abbia correttamente respinto l'accesso civico alla documentazione richiesta.

Ciò in quanto, tenendo conto della tipologia e della natura dei dati e delle informazioni personali contenuti nella documentazione oggetto dell'istanza di accesso civico, nel caso in esame, la generale conoscenza dei dati e delle informazioni richieste potrebbe determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei soggetti controinteressati, con possibili ripercussioni negative sul piano lavorativo, professionale, personale e sociale (cfr. par. 8.1 delle Linee guida dell'ANAC in materia di accesso civico, cit.). L'ostensione richiesta, unita peraltro al particolare regime di pubblicità dei dati oggetto di accesso civico e al ristretto ambito territoriale del Comune interessato di soli 4000 abitanti, può arrecare ai soggetti controinteressati, a seconda delle ipotesi e del contesto in cui le informazioni fornite possono essere utilizzate da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Parere Garante: n. 1 del 03/01/2019

Fattispecie: il parere del Garante, previsto dall'art. 5, comma 7, del d. lgs. n. 33 del 14 marzo 2013, nell'ambito del procedimento relativo a una richiesta di riesame di un provvedimento di diniego di una richiesta di accesso civico generalizzato avente ad oggetto la «copia nel formato detenuto da questa amministrazione (o in subordine in forma riassuntiva), contenente i dati del committente, descrizione dell'intervento, località del cantiere e tecnico progettista, delle **Segnalazioni Certificate di Inizio Attività (SCIA)** e possibilmente anche delle **Comunicazioni Inizio Attività Asseverata (CILA)** concernenti l'attività degli interventi edili da attuarsi nel territorio comunale, presentate nel mese di settembre 2018».

L'amministrazione ha negato l'accesso civico ai dati personali richiesti alla luce del limite, previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013, relativo all'esistenza di un pregiudizio concreto alla protezione dei dati personali dei soggetti interessati, richiamando in proposito il contenuto del parere già fornito dal Garante al medesimo Comune su altra richiesta di accesso civico identica, sotto il profilo soggettivo e oggettivo, alla presente (provv. n. 360 del 10/8/2017, in www.gdpd.it, doc. web n. [6969290](https://www.gdpd.it/Documenti/2017/08/360-10-08-2017)).

Quanto alle restanti informazioni, il Comune ha fornito al soggetto istante i dati relativi alle SCIA e CILA presentate all'ente nel periodo richiesto (senza comunicare dati personali), ossia la tipologia di titolo edilizio (SCIA o CILA), la descrizione dell'intervento (es: manutenzione straordinaria, installazione insegna; intervento miglioramento sismico, nuovo accesso carraio, variante in corso d'opera per ristrutturazione edilizia; opere interne; variante in corso d'opera, ecc.), le informazioni relative all'effettuazione dell'intervento nel comune o in una sua frazione.

Il soggetto istante, non ritenendosi soddisfatto dal riscontro ricevuto – lamentando di non aver ricevuto gli ulteriori dati personali (nomi, cognomi e indirizzi) – ha presentato richiesta di riesame del provvedimento di diniego dell'accesso civico al responsabile della prevenzione della corruzione e della trasparenza,

Contenuto del parere :

Il Garante rinvia al proprio parere n. 360 del 10/08/2017, salvo a precisare quanto di seguito riportato in merito al mancato bilanciamento fra gli interessi sottostanti, poiché, secondo l'istante, «la tutela del dato personale deve essere applicata alla luce del principio di proporzionalità nel bilanciamento con altri diritti e valori fondamentali, tra cui vi rientra quello alla trasparenza amministrativa e all'accesso ai documenti», principio che non sarebbe stato rispettato dal Comune nel non fornire i dati personali degli interessati che hanno presentato le SCIA e le CILA oggetto della richiesta di accesso civico generalizzato.

Sul bilanciamento fra trasparenza amministrativa e diritto alla protezione dei dati personali

La normativa statale in materia di trasparenza e accesso civico è chiara nello stabilire i presupposti (soggettivi e oggettivi) per l'esercizio del diritto di accesso civico – effettuando il bilanciamento fra gli interessi e valori fondamentali sopra descritti (trasparenza amministrativa e diritto alla protezione dei dati personali) – laddove prevede che «chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto», a meno che ciò non comporti un pregiudizio concreto alla tutela dell'interesse alla protezione dei dati personali, in conformità con la disciplina legislativa in materia (artt. 5, comma 2; 5-bis, comma 2, lett. a, del d. lgs. n. 33/2013).

Questo significa che, laddove una pubblica amministrazione riceva una richiesta di accesso civico a dati personali (o a documenti che ne contengano), e gli stessi non siano oggetto di pubblicazione obbligatoria, la stessa è tenuta in primo luogo a verificare se dall'ostensione dei predetti dati possa derivare un pregiudizio concreto alla protezione dei dati personali del/i soggetto/i a cui gli stessi si riferiscono, e in tal caso a rifiutarne l'accesso civico (cfr. a tal proposito anche il par. 8.1. delle Linee guida dell'ANAC).

Per effettuare la valutazione descritta, l'amministrazione cui è indirizzata la richiesta di accesso civico è tenuta a coinvolgere i soggetti controinteressati (art. 5, comma 5, del d. lgs. n. 33/2013), anche al fine di consentirgli di presentare eventuale motivata opposizione. Tali motivazioni costituiscono «un indice della sussistenza di un pregiudizio concreto, la cui valutazione però spetta all'ente e va condotta anche in caso di silenzio del controinteressato», tenendo, altresì, in considerazione i criteri contenuti nelle richiamate Linee guida dell'ANAC in materia di accesso civico (in particolare par. 8.1 intitolato «I limiti derivanti dalla protezione dei dati personali»).

Per tale motivo, nello specifico caso in esame, non è condivisibile la tesi per la quale ci sarebbe stato uno «sbilanciamento» a danno del soggetto istante nel provvedimento di diniego del Comune, solo perché – oscurando i dati personali (nomi, cognomi e indirizzo) dei controinteressati – «la tutela del dato personale» non sarebbe stata «applicata alla luce del principio di proporzionalità nel bilanciamento con altri diritti e valori fondamentali, tra cui vi rientra quello alla trasparenza amministrativa e all'accesso ai documenti». Come già evidenziato in altre sedi, non è possibile accordare una generale prevalenza della trasparenza o del diritto di accesso civico "generalizzato" a scapito di altri diritti ugualmente riconosciuti dall'ordinamento (quali quello alla riservatezza e alla protezione dei dati personali), in quanto, procedendo in tal modo, si vanificherebbe proprio il necessario bilanciamento degli interessi in gioco che richiede un approccio equilibrato nella ponderazione dei diversi diritti coinvolti, tale da evitare che i diritti fondamentali di eventuali controinteressati possano essere invece gravemente pregiudicati dalla messa a disposizione a terzi – non adeguatamente ponderata – di dati, informazioni e documenti che li riguardano (cfr.

prov. n. 521/2016, cit.). In caso contrario, vi sarebbe infatti il rischio di generare comportamenti irragionevoli in contrasto, per quanto attiene alla tutela della riservatezza e del diritto alla protezione dei dati personali, con la disciplina internazionale ed europea in materia (art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, Dir. 95/46/CE, Reg. (UE) 27/4/2016 n. 2016/679).

Il Garante ritiene che, ai sensi della normativa vigente e delle indicazioni contenute nelle Linee guida dell'ANAC, conformemente ai precedenti orientamenti di questa Autorità, **il Comune, abbia correttamente respinto l'istanza di accesso civico ai dati personali richiesti.**

Parere Garante: n. 29 del 07/02/2019

Fattispecie: Il caso sottoposto all'attenzione del Garante riguarda la presentazione di una richiesta di accesso civico a una specifica **comunicazione fornita al Comune di da un proprio dipendente**, contenente dati personali dello stesso, nonché ulteriori informazioni relative anche alla capacità professionale, alle prospettive di carriera e a iniziative svolte all'esterno all'amministrazione di appartenenza.

Contenuto parere: Il Comune - secondo il Garante - ha correttamente respinto l'accesso civico, considerando che l'ostensione del documento richiesto può arrecare proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Infatti, considerata la tipologia e la natura dei dati e delle informazioni personali oggetto dell'istanza di accesso e il particolare regime di pubblicità dei dati oggetto di accesso civico, si ritiene che dall'ostensione dei dati e delle informazioni richieste potrebbero derivare al soggetto interessato ripercussioni negative sul piano sociale, relazionale e professionale. Ciò anche pensando alle ragionevoli aspettative di confidenzialità dell'interessato e alla non prevedibilità delle conseguenze derivanti a quest'ultimo dalla conoscibilità da parte di chiunque dei dati richiesti (cfr. par. 8.1 delle Linee guida dell'ANAC in materia di accesso civico, cit.).

Le predette osservazioni impediscono, come evidenziato anche dal Comune, la possibilità di accordare un eventuale accesso civico parziale oscurando i dati del controinteressato, ai sensi dell'art. 5-bis, comma 4, del d. lgs. n. 33/2013, in quanto tale accorgimento tecnico non eliminerebbe completamente la possibilità di risalire, atteso che questi potrebbe essere facilmente identificato, anche da parte di terzi, attraverso il complesso della vicenda descritta e le ulteriori informazioni contenute nel documento di cui è stata chiesta l'ostensione.

Parere Garante: n. 145 del 26/06/2019

Fattispecie: riesame rigetto accesso civico ex art. 5, comma 2, d.lgs. n. 33/2013, relativo ad «atti e documenti da cui si evincano i provvedimenti adottati nei confronti degli amministratori locali (sindaco, vice sindaco, assessori, e Presidente consiliare) destinatari della **rideterminazione delle indennità spettanti agli Amministratori locali per il periodo gennaio/maggio 2012] e volti al recupero delle eccedenze**», compreso «i pagamenti dagli stessi eseguiti a titolo di restituzione».

Contenuto del parere: Il Garante invita il Comune a rivalutare la richiesta di accesso civico ai documenti richiesti, previo coinvolgimento dei soggetti controinteressati, fornendo nella risposta – eventualmente affermativa, negativa o parzialmente tale – una motivazione congrua e completa rispetto all'esistenza o meno del limite di cui all'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013, tenendo conto dei seguenti elementi favorevoli all'ostensione:

1. della circostanza che alcune informazioni sono già state oggetto di pubblicazione obbligatoria (es.: il mancato rispetto del patto di stabilità interno per l'anno 2011 e la determinazione della restituzione di parte delle indennità spettanti agli allora amministratori locali);
2. del ruolo, della funzione pubblica e dell'attività di pubblico interesse esercitata dagli amministratori locali cui si riferiscono i dati personali oggetto di accesso civico, al fine di verificare una "reale" esistenza del pregiudizio alla protezione dei dati personali di soggetti titolari di incarichi istituzionali;
3. del regime di pubblicità e trasparenza rafforzato richiesto per coloro che rivestono incarichi di indirizzo politico in relazione ai compensi percepiti (cfr. art. 14 d. lgs. n. 33/2013) e dell'attenuata aspettativa di confidenzialità in capo a coloro che rivestono o hanno rivestito incarichi pubblici quali gli amministratori di un ente locale, anche se di ridotte dimensioni e con popolazione minore di 15.000 abitanti.

Nell'effettuare la predetta valutazione circa la possibilità di fornire tutti i dati personali richiesti deve in ogni caso:

4. essere rispettato il principio di «minimizzazione» dei dati personali (art. 5, par. 1, lett. c, RGPD), alla luce del quale i dati personali eventualmente forniti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità di trasparenza propria dell'istituto dell'accesso civico, in modo che non si realizzi un'interferenza ingiustificata e sproporzionata nei diritti e libertà delle persone;
5. tenersi conto dell'eventuale esistenza di contenziosi giudiziari ancora in corso, che possono essere stati attivati dai soggetti controinteressati in merito alla richiesta di restituzione di parte delle indennità percepite e l'interferenza che la conoscibilità di questi dati potrebbe determinare sul diritto di difesa.

Parere Garante: n. 200 del 07/12/2019

Fattispecie: oggetto dell'accesso civico risultano essere «Copie degli **elaborati delle prove scritte, dei relativi verbali di correzione e dei curriculum vitae sottoposti da tutti i candidati** nell'ambito della procedura concorsuale per l'accesso al 33° ciclo del corso di dottorato di ricerca in Scienze della Formazione e Psicologia».

Non sono stati coinvolti i soggetti controinteressati. L'istante ha chiesto il riesame del diniego all'accesso.

Contenuto parere: Il Garante ritiene che l'amministrazione abbia correttamente respinto l'accesso civico ai documenti richiesti, per le seguenti motivazioni:

In primo luogo, per gli specifici profili inerenti all'accesso civico alla copia degli elaborati scritti di un concorso pubblico, si deve tenere presente che tali documenti, in generale, sono indicativi di molteplici aspetti di carattere personale circa le caratteristiche individuali, relativi ad esempio alla preparazione professionale, alla cultura, alle capacità di espressione, o al carattere del candidato, che costituiscono aspetti valutabili nella selezione dei partecipanti. Inoltre, in alcuni casi, e a seconda della traccia sottoposta, il contenuto degli elaborati è capace di rivelare anche informazioni e convinzioni che possono rientrare nelle «categorie particolari di dati personali» di cui all'art. 9, par. 1, del Regolamento (si pensi, in particolare, a elaborati nei quali potrebbero evincersi «opinioni politiche», «convinzioni filosofiche o di altro genere»).

Analogamente si osserva che i contenuti generalmente inseriti nel curriculum vitae sono molteplici e la relativa ostensione può consentire l'accesso, a seconda di come è redatto il cv, a numerosi dati (es.: nominativo, data e luogo di nascita, residenza, telefono, e-mail, nazionalità) e informazioni di carattere personale (es.: esperienze e competenze professionali, istruzione e formazione, competenze personali, competenze comunicative, competenze organizzative e gestionali, pubblicazioni, presentazioni, progetti, conferenze, seminari, riconoscimenti e premi, appartenenza a gruppi/associazioni, referenze, menzioni, corsi, certificazioni, ecc.), che per motivi individuali non sempre si desidera portare a conoscenza di soggetti estranei.

Tenuto quindi conto che «Tutti i documenti, le informazioni e i dati oggetto di accesso civico [...] sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7», pur nel rispetto dei limiti derivanti dalla normativa in materia di trattamento dei dati personali per ogni ulteriore trattamento (art. 3, comma 1, del d. lgs. n. 33/2013), l'ostensione dei documenti richiesti è suscettibile di determinare, a seconda delle ipotesi e del contesto in cui possono essere utilizzati da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Pertanto, si ritiene che, ai sensi della normativa vigente e delle indicazioni contenute nelle Linee guida dell'ANAC in materia di accesso civico, considerando la natura dei dati personali coinvolti e il particolare regime di pubblicità dei dati e documenti oggetti di accesso civico – conformemente ai precedenti orientamenti del Garante in materia di accesso civico agli elaborati scritti dei candidati ad un concorso pubblico e/o a curricula vitae presentati dai candidati (cfr. pareri n. 162 del 30 marzo 2017, doc. web. n. [6393422](#); n. 246 del 24 maggio 2017, doc. web. n. [6495600](#); n. 366 del 7 settembre 2017, doc. web. n. [7155171](#); n. 433 del 26 ottobre 2017, doc. web. n. [7156158](#)).

Parere Garante : n. 220 del 18/12/2019

Fattispecie : parere previsto dall'art. 5, comma 7, del d. lgs. n. 33/2013, nell'ambito del procedimento relativo a una richiesta di riesame sul provvedimento di diniego di un accesso civico

Oggetto dell'istanza: l'istanza di accesso civico generalizzato aveva a oggetto «tutti i **verbali di abusi edilizi ed i relativi provvedimenti adottati**, anni 2018 e 2019, anche previo oscuramento dei dati personali e dei dati sensibili».

Contenuto del parere: Un'eventuale ostensione delle informazioni riferite ai soggetti destinatari di provvedimenti di accertamento di irregolarità edilizie potrebbe, infatti, causare a questi ultimi ripercussioni negative, anche sul piano sociale e relazionale, considerando peraltro – come evidenziato dal Comune – che sono ancora pendenti i procedimenti penali avviati a seguito degli abusi edilizi. In caso di accoglimento dell'istanza, si determinerebbe quindi un'interferenza sproporzionata nei diritti e libertà dei soggetti controinteressati in violazione del principio di «minimizzazione dei dati» contenuto nel RGPD, in base al quale i dati personali devono essere, fra l'altro, «limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, par. 1, lett. c). Ciò anche tenendo conto della ragionevole aspettativa di confidenzialità e della non prevedibilità delle conseguenze derivanti dalla conoscibilità da parte di chiunque della documentazione richiesta (cfr. par. 8.1 delle Linee guida dell'ANAC in materia di accesso civico, cit.).

Le predette considerazioni impediscono, altresì, di accordare un eventuale accesso civico parziale ai sensi dell'art. 5-bis, comma 4, del d. lgs. n. 33/2013, oscurando i nominativi dei soggetti controinteressati – come richiesto nell'istanza di accesso civico – in quanto questi ultimi riceverebbero in ogni caso un pregiudizio alla protezione dei propri dati personali, risultando indirettamente identificabili attraverso le informazioni di dettaglio o gli ulteriori dati di contesto, contenuti nei documenti richiesti (es.: dati catastali, indirizzi e numeri civici, etc.), anche tenendo conto del ristretto ambito territoriale del Comune interessato di soli 8600 abitanti circa.

.... non sussistono, invece, ragioni attinenti alla protezione dei dati personali dei controinteressati (ai sensi dell'art. 5-bis, comma 2, lett. a, del d. lgs. n. 33/2013) in relazione all'eventuale ostensione al soggetto richiedente – allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico – di “dati aggregati” (privi di dati identificativi e di ogni ulteriore informazione che può identificare i soggetti controinteressati anche indirettamente), quali – ad esempio – il numero degli abusi edilizi rilevati negli ultimi due anni e le aree/zone comunali interessate prive di indirizzi e numeri civici.

Parere Garante: n. 5 del 23/01/2020

Fattispecie: oggetto dell'accesso civico generalizzato risulta essere la “**denuncia/querela/segnalazione nella sua interezza**, ivi compresi eventuali allegati”, fatta da un cittadino al fine di far rimuovere la pianta, di proprietà dell'istante, posizionata in un vicoletto rientrate in un'area pedonale perimetrata, nonché “l'atto autorizzativo – nella sua interezza, ivi compresi anche gli eventuali allegati [...] rilasciato al motociclo targato [...] per l'accesso e la circolazione” nel vicoletto sopra citato. Il Comune ha respinto l'istanza di accesso civico.

Contenuto del parere: Deve in primo luogo essere ricordato che i dati e i documenti che si ricevono a seguito di una istanza di accesso civico – a differenza di quelli che si ricevono tramite l'accesso ai documenti amministrativi ai sensi della legge n. 241 del 7/8/1990 – divengono «pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7», sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, del d. lgs. n. 33/2013).

Di conseguenza, è anche alla luce di tale amplificato regime di pubblicità dell'accesso civico che va valutata l'esistenza di un possibile pregiudizio concreto alla protezione dei dati personali dei soggetti controinteressati, in base al quale decidere se rifiutare o meno l'accesso ai documenti richiesti.

Ciò anche tenendo conto delle ragionevoli aspettative di confidenzialità dell'interessato e alla non prevedibilità delle conseguenze derivanti a quest'ultimo dalla conoscibilità da parte di chiunque dei dati richiesti (cfr. par. 8.1 delle Linee guida dell'ANAC in materia di accesso civico, cit.).

La valutazione dell'ostensione di dati personali nell'ambito del procedimento di accesso civico, deve inoltre essere effettuata anche nel rispetto dei principi indicati dall'art. 5 del RGPD, fra cui quello di «minimizzazione dei dati», secondo il quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, par. 1, lett. c), in modo che non si realizzi un'interferenza ingiustificata e sproporzionata nei diritti e libertà delle persone cui si riferiscono tali dati (cfr. anche art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; art. 8 della Carta dei diritti fondamentali dell'Unione europea e della giurisprudenza europea in materia).

Pertanto, il riconoscimento di un accesso civico generalizzato ai documenti contenenti dati personali sopradescritti, unito alla generale conoscenza e al particolare regime di pubblicità dei dati oggetto di accesso civico, può costituire un'interferenza sproporzionata nei diritti e libertà del controinteressato, arrecando a quest'ultimo, a seconda delle ipotesi e del contesto in cui i dati e le informazioni fornite possono essere utilizzate da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013. Al riguardo, si ritiene che, ai sensi della normativa vigente e delle indicazioni contenute nelle Linee guida dell'ANAC in materia di accesso civico, conformemente ai precedenti orientamenti del Garante (cfr. pareri n. 220 del 18 dicembre 2019, in www.gpdp.it, doc. web n. [9232553](#); n. 187 del 10 ottobre 2019, in www.gpdp.it, doc. web n. [9198109](#); n. 179 del 2 ottobre 2019, in www.gpdp.it, doc. web n. [9162546](#)) – l'amministrazione abbia correttamente respinto l'accesso civico ai documenti richiesti.

Parere Garante: n. 6 del 23/01/2020

Fattispecie: istanza di accesso civico generalizzato al “**Ruolo matricolare Comunale dei Militari**”. Mod. DE/002E», dall'anno 1950 al 1985. Nella richiesta è indicato che la finalità dell'accesso risiede nella volontà di contattare i soggetti contenuti nei predetti registri potenzialmente interessati, in «previsione di una loro eventuale adesione associativa».

il Comune ha negato l'accesso civico, richiamando il limite della protezione dei dati personali contenuto nell'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Si tratta di una mole di dati e informazioni personali riferibili a dati comuni e, in alcuni casi, anche a “categorie particolari di dati personali” (art. 9, RGPD) appartenenti a circa 170.000 soggetti interessati. I registri richiesti, infatti, riportano «nominativi, data e luogo di nascita, informazioni in ordine alla residenza alla data di registrazione, unità militare di assegnazione, grado rivestito, data di congedo», nonché «annotazioni spesso coinvolgenti profili attinenti alla salute, in ordine all'eventuale esonero permanente dal servizio militare obbligatorio (riformato per ...), unitamente ad indicazioni circa la condizione di obiettore di coscienza e di eventuale, successiva rinuncia al relativo status [...] si per sé sintomatiche di opinioni politiche e/o di convinzioni religiose o filosofiche».

Il Garante evidenzia che i dati e i documenti che si ricevono a seguito di una istanza di accesso civico divengono

«pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7», sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, del d. lgs. n. 33/2013).
La valutazione dell'ostensione di dati personali nell'ambito del procedimento di accesso civico, deve inoltre essere effettuata anche nel rispetto dei principi indicati dall'art. 5 del RGPD, fra cui quello di «limitazione della finalità» e di «minimizzazione dei dati» (art. 5, par. 1, lett. b e c), in modo che non si realizzi un'interferenza ingiustificata e sproporzionata nei diritti e libertà delle persone cui si riferiscono tali dati (cfr. anche art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; art. 8 della Carta dei diritti fondamentali dell'Unione europea e della giurisprudenza europea in materia).
In tale quadro, Il Garante ritiene che il Comune – seppur con una succinta motivazione – abbia correttamente negato l'accesso civico ai registri del "Ruolo matricolare Comunale dei Militari".

Parere Garante : n. 57 del 16/03/2020

Fattispecie : parere previsto dall'art. 5, comma 7, del d. lgs. n. 33/2013, nell'ambito del procedimento relativo a una richiesta di riesame sul provvedimento di diniego di un accesso civico

Oggetto dell'istanza: copia degli **elenchi mensili dei rapporti comunicati dagli organi di Polizia riguardanti opere e lottizzazioni abusive** prodotti durante le annualità 2016 – 2017 – 2018 e 2019, ai sensi dell'art. 31 del D.P.R. 6 giugno 2001.

Contenuto del parere: si ricorda che la normativa statale di settore già prevede specifici obblighi di pubblicità in materia di opere abusive, laddove è sancito che «Il segretario comunale redige e pubblica mensilmente, mediante affissione nell'albo comunale, i dati relativi agli immobili e alle opere realizzati abusivamente, oggetto dei rapporti degli ufficiali ed agenti di polizia giudiziaria e delle relative ordinanze di sospensione e trasmette i dati anzidetti all'autorità giudiziaria competente, al presidente della giunta regionale e, tramite l'ufficio territoriale del governo, al Ministro delle infrastrutture e dei trasporti» (art. 31, comma 7, del d.P.R. n. 380 del 6/6/2001).

In merito al citato obbligo, occorre però ricordare che l'art. 31, comma 7, del d.P.R. n. 380/2001, non specifica nel dettaglio quali dati relativi agli immobili e alle opere realizzati abusivamente (oggetto dei rapporti degli ufficiali ed agenti di polizia giudiziaria e delle relative ordinanze di sospensione), bisogna pubblicare. Inoltre, i dati sono mantenuti online per periodi di tempo limitati e rimossi una volta raggiunti gli scopi per i quali sono stati resi pubblici.

... **nulla osta all'ostensione tramite l'istituto dell'accesso civico generalizzato dei dati resi pubblici in virtù di un obbligo di pubblicazione online**, chiaramente nel rispetto dei citati principi di limitazione della finalità e di minimizzazione dei dati contenuti nell'art. 5, par. 1, lett. b) e c), del RGPD (cfr. anche le indicazioni fornite da Garante nel provvedimento n. 243 del 15 maggio 2014 recante le «Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati», in G.U. n. 134 del 12 giugno 2014, doc. web n. [3134436](#)).

Sotto tale profilo, **non sussistono impedimenti legati alla protezione dei dati personali con riferimento all'ostensione di dati e informazioni quali, ad esempio, il numero di protocollo del rapporto, la data, l'organo da cui proviene il rapporto, la località, il tipo di abuso, gli estremi dell'ordinanza di sospensione**.

Quanto invece agli altri dati personali, come il nominativo del proprietario committente e l'indirizzo, si rappresenta che un'eventuale ostensione tramite l'istituto dell'accesso civico – tenendo conto del relativo regime di pubblicità e della riutilizzabilità dei dati da parte di terzi – potrebbe causare effetti sfavorevoli sui soggetti controinteressati, considerando che, in alcuni casi, potrebbe essere ancora pendente un giudizio penale o si potrebbero fornire informazioni risalenti nel tempo (dal 2016), riguardanti procedure magari già definite, realizzando in tal modo quel pregiudizio concreto alla tutela della protezione dei dati personali del controinteressato, previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Si invita il Comune a rivalutare la richiesta di accesso civico, fornendo nella risposta «una congrua e completa, motivazione» con riferimento ai limiti derivanti dalla protezione dei dati personali (cfr. Linee guida dell'ANAC, par. 5.3), valutando la possibilità di accordare un eventuale accesso civico parziale ai sensi dell'art. 5-bis, comma 4, del d. lgs. n. 33/2013, mediante oscuramento – anche a seguito del coinvolgimento dei soggetti controinteressati nel procedimento, ai sensi dell'art. 5, comma 5, del d. lgs. n. 33/2013 – del nominativo del proprietario committente e dell'indirizzo.

Parere Garante: n. 147 del 29/07/2020

Fattispecie: richiesta di accesso civico – ai sensi dell'art. 5 comma 2, del d. lgs. n. 33/2013 – avente a oggetto il rilascio di copia «delle **schede di valutazione compilate dal Sindaco nell'anno 2019, relative ai comportamenti organizzativi dei Dirigenti/Direttori per l'anno 2018**», nonché **dei «punteggi finali e totali in percentuale**, attribuiti ai Dirigenti/Direttori, relativi all'indennità di risultato per l'anno 2018».

Violazioni accertate:

premessa: L'amministrazione ha effettuato la comunicazione ai soggetti controinteressati (art. 5, comma 5, d. lgs. n. 33/2013), i quali si sono opposti evidenziando il contenuto strettamente personale della documentazione richiesta e l'inopportunità della relativa comunicazione a terzi stante la potenziale diffusione. Un controinteressato ha evidenziato, inoltre, che le esigenze conoscitive strumentali al perseguimento delle finalità dell'accesso civico, con riferimento ai dirigenti, sarebbero già soddisfatte dai previsti obblighi di pubblicazione online degli emolumenti complessivamente percepiti a carico della finanza pubblica e dei dati relativi alla valutazione della performance e alla distribuzione dei premi al personale (art. 14, comma 1-ter; e 20, del d. lgs. n. 33/2013).

Il Comune ha accordato un accesso parziale, consentendo l'ostensione della «parte riguardante i punteggi finali e totali» (fornendo al riguardo il link del sito web istituzionale su cui sono stati pubblicati tali dati), ma ha invece negato l'accesso alla «copia della scheda di valutazione compilata dal Sindaco nell'anno 2019, relativa ai comportamenti organizzativi dei Dirigenti/Direttori per l'anno 2018», in quanto «tutti i soggetti contro-interessati hanno comunicato la loro opposizione alla [...] richiesta, stante il contenuto prettamente personale delle schede di valutazione in parola, del quale non si è ritenuto opportuno che venisse reso noto a terzi e, potenzialmente, anche diffuso».

violazioni: il Comune ha correttamente respinto l'accesso civico alla «copia delle schede di valutazione compilate dal Sindaco nell'anno 2019, relative ai comportamenti organizzativi dei Dirigenti/Direttori per l'anno 2018, in quanto la relativa ostensione, anche considerando il particolare regime di pubblicità dei dati e delle informazioni ricevute tramite l'istituto dell'accesso civico (cfr. art. 3, comma 1, d. lgs. n. 33/2013), potrebbe determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei dirigenti controinteressati, arrecando a questi ultimi proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013. Infatti, un eventuale accoglimento dell'accesso civico potrebbe determinare ripercussioni negative sul piano professionale, personale, sociale e relazionale, sia all'interno che all'esterno dell'ambiente lavorativo di questi ultimi; esponendoli a possibili difficoltà relazionali con i colleghi di lavoro e creando potenziali pregiudizi da parte degli utenti esterni con cui potrebbero venire a contatto nell'esercizio delle loro funzioni.

Sanzione: nessuna

Parere Garante: n. 58 dell'11/02/2021

Fattispecie: il Difensore civico della Regione ha chiesto al Garante il parere previsto dall'art. 5, comma 8, del d. lgs. n. 33/2013, nell'ambito del procedimento relativo a un ricorso a esso presentato su un provvedimento di diniego di un'istanza di accesso civico che aveva a oggetto la **«copia della relazione sulla gestione della funzione di polizia locale redatta dal Presidente dell'Unione », che risulta essere stata letta «nella seduta del Consiglio Comunale di ... del ... ».**

Il Comune di nel provvedimento di diniego ha rappresentato al soggetto istante che la predetta relazione «contiene apprezzamenti sulla condotta di persone e ripetuti riferimenti a dati personali (anche sensibili)» e che tale circostanza sarebbe «comprovata dal fatto che la lettura è avvenuta nel corso di una seduta di consiglio comunale non aperta al pubblico, in ossequio al disposto di cui all'art. 10, comma 11, dello Statuto comunale». Per tale motivo, è stato rifiutato l'accesso civico, ritenendo sussistere il limite di cui all'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013, «stante la necessità di evitare un pregiudizio concreto alla tutela dell'interesse privato alla protezione dei dati personali». Ciò «in ragione del fatto che tale documento (classificato come riservato) contiene dati e informazioni che, pur riguardando l'attività e l'organizzazione della Pubblica Amministrazione, sono inscindibilmente commisti a dati di carattere personale meritevoli di tutela ai sensi della normativa in materia di protezione dei dati personali».

Nello specifico, vi sono numerosi riferimenti a soggetti a vario titolo citati nel documento oggetto di accesso civico, nonché intere pagine dedicate alla puntuale e dettagliata descrizione di condotte e fatti oggetto di indagine e accertamento giudiziario e amministrativo, ancora in corso. Sono, inoltre, riportate risultanze e verbali di audizioni interne all'amministrazione sui predetti fatti, comprensive della trascrizione integrale delle domande poste e delle relative dichiarazioni rilasciate dalle persone coinvolte.

La predetta relazione si riferisce a numerosi soggetti controinteressati, che non risultano coinvolti nel procedimento di accesso civico.

Contenuto del parere : la relativa ostensione, anche considerando il particolare regime di pubblicità dei dati e informazioni che si ricevono tramite l'istituto dell'accesso civico (cfr. art. 3, comma 1, d. lgs. n. 33/2013), avrebbe determinato un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei soggetti controinteressati a vario titolo citati nel documento oggetto di accesso civico, anche con riferimento a possibili interferenze con gli accertamenti e le indagini giudiziarie, nonché amministrative, in corso che potrebbero derivare dalla pubblicità e dalla conoscenza generalizzata dei fatti e delle dichiarazioni ivi riportate, arrecando proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Infatti, tenuto conto della tipologia e della natura dei dati e delle informazioni personali, anche di dettaglio,

contenuti nella relazione sulla polizia locale richiesta, e prima descritti, un eventuale accoglimento dell'accesso civico avrebbe determinato ripercussioni negative sul piano professionale, personale, sociale e relazionale dei soggetti a vario titolo coinvolti. Bisogna, inoltre, tener conto delle ragionevoli aspettative di confidenzialità dei controinteressati in relazione al trattamento dei propri dati personali al momento in cui questi sono stati raccolti dal titolare del trattamento, nonché della non prevedibilità, al momento della raccolta dei dati, delle conseguenze derivanti dall'eventuale conoscibilità da parte di chiunque del documento richiesto richiesti tramite l'accesso civico (cfr. par. 8.1 delle Linee guida dell'ANAC in materia di accesso civico, cit.).

La presenza, nella documentazione richiesta, di dati e informazioni dettagliati dei soggetti a vario titolo interessati, impedisce inoltre di poter accordare anche un eventuale accesso civico parziale ai sensi dell'art. 5-bis, comma 4, del d. lgs. n. 33/2013; oscurando, ad esempio, i relativi dati identificativi (nome e cognome). Tale accorgimento, infatti, non elimina la possibilità che il/i soggetto/i controinteressato/i possa/no essere identificato/ti indirettamente tramite gli ulteriori dati di contesto contenuti nel documento richiesto o da altre informazioni nella disponibilità di terzi. A tale riguardo, occorre infatti ricordare che – ai sensi del RGPD – «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, n. 1).

Provvedimento Garante : n. 281 del 22/07/2021

Fattispecie : pubblicazione nell'Albo pretorio, nel Registro degli accessi e nella sezione "Amministrazione trasparente" del documento contenente – **oltre i dati del professionista incaricato** – incidentalmente **anche i dati personali di un soggetto terzo estraneo alla dichiarazione**, ossia il reclamante sig. XX (quali relativo nominativo, residenza e informazioni inerenti alla presentazione di un ricorso contro il comune per l'annullamento di un ordinanza sindacale di inagibilità);

Violazioni : l'illiceità del trattamento di dati personali effettuato dal Comune di, in quanto:

- 1) la diffusione dei dati personali del reclamante contenuti nel documento intitolato «XX» di un altro professionista, sopra identificato ..., è in contrasto con il principio di «minimizzazione» dei dati, che non risultano «limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (ossia la trasparenza dell'«attestazione dell'avvenuta verifica dell'insussistenza di situazioni, anche potenziali, di conflitto di interessi» del consulente/collaboratore dell'ente), in violazione dell'art. 5, par. 1, lett. c), del RGPD;
- 2) la diffusione dei dati personali del reclamante e degli altri soggetti interessati che hanno inoltrato richieste di accesso al Comune — contenuti nel documento, nonché nel «XX» presenti nella sezione Amministrazione trasparente, agli url indicati nelle lettere da a) ad h) del medesimo paragrafo — risulta avvenuta in assenza di idonei presupposti normativi, in violazione dell'art. 2-ter, commi 1 e 3, del Codice (e in maniera non conforme alle indicazioni contenute nelle Linee guida dell'ANAC e nella Circolare della funzione pubblica sopra richiamate al par. 2); nonché dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD.

Sanzione: euro 2.200,00

ACCESSO DOCUMENTALE

Parere Garante n. 115 del 23/05/2019

Fattispecie: la richiesta di accesso civico riguarda dati, informazioni e documenti contenenti un gran numero di dati personali riferiti a più di 1700 unità, di specie differente, riguardanti, in particolare, **la lista del personale utilizzato nei vari servizi, il curriculum vitae del personale, la documentazione comprovante il possesso dei titoli, competenze ed esperienze previste per le varie figure professionali, la documentazione richiesta per il personale addetto allo specifico servizio identificato in atti** e, in ogni caso «Ogni altro atto e/o documento prodotto in fase di partecipazione e di offerta tecnica atto a dimostrare l'idoneità organizzativa tecnica e professionale degli aggiudicatari e del personale impiegato».

il Ministero ha negato l'accesso civico, evidenziando il coinvolgimento di «una mole consistente di soggetti terzi, aventi immediato e diretto riflesso sull'identità, il domicilio, i recapiti (residenziali e telefonici), sullo stato familiare, attitudini e capacità culturali, professionali e lavorative. L'ostensione dei curricula vitae del personale addetto ai servizi oggetto di gara non può che comportare, pertanto, una immediata e diretta compressione del diritto alla riservatezza dei dati personali, posto che, nella documentazione di cui si chiede l'accesso, sono presenti informazioni sensibili». L'amministrazione ha, inoltre, eccepito il carattere massivo della richiesta di accesso – anche considerando che gli «atti e documenti di cui si chiede l'ostensione sono relativi ai soggetti impiegati nell'espletamento dei servizi

in appalto che superano le 1.700 unità» – idoneo a «“paralizzare” per un periodo di tempo significativo l’intero Ufficio con compromissione dei servizi istituzionali».

Violazioni accertate:

premessa: , la fattispecie sottoposta all’attenzione del Garante – come rilevato dalla più recente giurisprudenza amministrativa (cfr. TAR Lazio, Roma, sez. II, 14/01/2019, n. 425; TAR Lombardia, Milano, sez. I, n. 630; TAR Marche, Ancona, sez. I, 18/10/2018, n. 677; TAR Emilia Romagna, Parma, sez. I, 18/07/2018, n. 197; TAR Puglia, Lecce, sez. II, 12/04/2019, n. 599; cfr. anche TAR, Toscana, sez. III, 17/04/2019 N. 577) – ricade in una delle ipotesi di “esclusione” dell’accesso civico generalizzato, considerando che «Il diritto di cui all’articolo 5, comma 2, è escluso nei [...] casi in cui l’accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all’articolo 24, comma 1, della legge n. 241 del 1990» (art. 5-bis, comma 3, del d. lgs. n. 33/2013).

La giurisprudenza ritiene che «l’accesso agli atti concernenti la procedura di affidamento e la fase di esecuzione dei contratti pubblici è oggetto di una disciplina ad hoc, costituita dalle apposite disposizioni contenute nel Codice dei contratti pubblici e, ove non derogate, da quelle in tema di accesso ordinario recate dalla legge n. 241 del 1990. In tale ambito non trova perciò applicazione l’istituto dell’accesso civico generalizzato, stante la clausola di esclusione contenuta nel richiamato articolo 5- bis, comma 3, del decreto legislativo n. 33 del 2013» (sent. TAR Lazio n. 425/2019, cit.). La scelta del legislatore ... coinvolge interessi privati di natura economica e imprenditoriale di per sé sensibili (e quindi astrattamente riconducibili alla causa di esclusione di cui al comma 2, lett. c), dell’art. 5-bis del d.lgs. n. 33 del 2013), specie quando tali interessi, dopo l’aggiudicazione, vanno a porsi su di un piano pari ordinato – assumendo la connotazione di veri e propri diritti soggettivi - rispetto a quelli della stazione committente” (così ancora TAR Parma, n. 197 del 2018, cit.)» (Ibidem).

Siccome, a differenza dei documenti a cui si è avuto accesso ai sensi della l. n. 241 del 7/8/1990, i dati e i documenti che si ricevono a seguito di una istanza di accesso civico generalizzato divengono «pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell’articolo 7», sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, del d. lgs. n. 33/2013). Anche alla luce di tale amplificato regime di pubblicità dell’accesso civico che va verificata l’esistenza di un possibile pregiudizio concreto alla protezione dei dati personali dei soggetti controinteressati, in base al quale decidere se rifiutare o meno l’accesso civico alle informazioni e ai documenti richiesti. La decisione sulla eventuale ostensione di dati personali nell’ambito del procedimento di accesso civico, deve inoltre tener conto anche nel rispetto dei principi indicati dall’art. 5 del Regolamento (UE) 2016/679 (RGPD), fra cui quello di «minimizzazione dei dati», secondo il quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, par. 1, lett. c), in modo che non si realizzi un’interferenza ingiustificata e sproporzionata nei diritti e libertà delle persone cui si riferiscono tali dati (cfr. anche art. 8 della Convenzione europea per la salvaguardia dei diritti dell’uomo e delle libertà fondamentali; art. 8 della Carta dei diritti fondamentali dell’Unione europea e della giurisprudenza europea in materia).

decisione: Si tratta di dati e informazioni, attinenti ad aspetti dettagliati della vita lavorativa che, in caso di accoglimento dell’istanza di accessocivico, diverrebbero pubblici e tendenzialmente riutilizzabili (cfr. art. 3, comma 1, del d. lgs. n. 33/2013); ma che, invece, per motivi individuali non sempre si desidera portare a conoscenza di soggetti estranei e consentire peraltro che vengano riutilizzati per altre finalità non conosciute né conoscibili al momento della loro acquisizione da parte del richiedente l’accesso. La relativa ostensione, inoltre, considerando anche la quantità e qualità dei dati personali coinvolti, può avere – in relazione ai casi e al contesto in cui possono essere utilizzate da parte di terzi estranei che non è dato conoscere a priori – possibili ripercussioni negative sul piano relazionale, personale, sociale dei soggetti controinteressati, sia all’interno che all’esterno dell’ambiente lavorativo (si pensi, ad esempio, a eventuali prospettive di impiego a cui gli interessati potrebbero aspirare in futuro), integrando proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall’art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013, alla luce del quale, ai sensi della normativa vigente e delle indicazioni contenute nelle Linee guida dell’ANAC, l’accesso civico va rifiutato (cfr. in senso conforme anche i precedenti orientamenti di questa Autorità in materia di accesso civico ai curriculum alle altre informazioni personali dei dipendenti: parere n. 162 del 30/3/2017, in www.gpdp.it, doc. web n. [6393422](#); n. 29 del 7/2/2019, ivi, doc. web n. [9086520](#); n. 485 del 29/11/2018, ivi, doc. web n. [9065367](#); n. 231 del 18/4/2018, ivi, doc. web n. [8983308](#); n. 421 dell’11/7/2018, ivi, doc. web n. [9037343](#); n. 466 dell’11/10/2018, doc. web n. [9063969](#)).

Le informazioni di dettaglio contenute nella documentazione richiesta, inoltre, impediscono di poter accordare anche un eventuale accesso civico parziale ai sensi dell’art. 5-bis, comma 4, del d. lgs. n. 33/2013; oscurando, ad esempio, i dati identificativi, di contatto e di residenza (nome e cognome, telefono, indirizzo) ivi contenuti. Tale accorgimento, infatti, non elimina la possibilità che i soggetti interessati siano re-identificati da soggetti terzi, anche all’interno dell’amministrazione stessa, tramite gli ulteriori dati di contesto contenuti nella documentazione richiesta.

Riguardo l’interesse personale dell’istante con cui è stato motivato anche la richiesta di accesso documentale, il Garante afferma che “Per questi aspetti, rimane impregiudicata ogni valutazione del Ministero in ordine alla verifica,

nel caso in esame, dell'esistenza di un interesse qualificato dell'istante e dei presupposti per l'esercizio del diverso diritto di accesso ai documenti amministrativi ai sensi degli artt. 22 ss. della citata legge n. 241/1990."

ALBO PRETORIO

Provvedimento Garante: n. 384 del 21/09/2017

Fattispecie: **ordinanza di demolizione delle opere realizzate abusivamente e ripristino dello stato dei luoghi**, contenente dati personali e fiscali dei ricorrenti nonché i dati catastali dell'immobile, pubblicata nella sezione "ordinanze" dell'Albo pretorio online per oltre due anni oltre il termine di pubblicazione obbligatoria.

Violazioni: il Comune di ha provveduto, sia pure dopo il decorso del termine di pubblicazione previsto dalla disciplina di settore, ad oscurare i dati identificativi dei ricorrenti all'interno dell'ordinanza sopra citata, attualmente conservata nella sezione archivio dell'albo pretorio on-line, disponendo altresì l'eliminazione della copia presente nella sezione ordinanze;

tuttavia, all'interno dell'ordinanza pubblicata nell'archivio dell'albo pretorio on-line, risultano tuttora visibili i dati catastali identificativi dell'immobile oggetto del provvedimento, come tali idonei ad identificare, sia pure indirettamente, gli interessati nella loro qualità di proprietari dello stesso;

pur essendo stati oscurati i dati direttamente identificativi di questi ultimi, effettuando una ricerca nominativa relativa a YY tramite i motori di ricerca esterni al sito istituzionale, risulta tuttora sussistente un collegamento con la pagina del sito istituzionale dell'ente contenente l'elenco riassuntivo delle ordinanze di tipo edilizio, ivi inclusa quella di cui sono stati destinatari i ricorrenti;

Considerato ...il grave pregiudizio derivante alla loro reputazione dovuto alla perdurante diffusione di dati personali che li riguardano in assenza di una norma di legge che la giustifichi, tenuto peraltro conto del fatto che "la questione della legittimità dell'ordinanza di che trattasi è attualmente sub iudice innanzi al Consiglio di Stato";

Il Garante accoglie parzialmente il ricorso e, per l'effetto, ordina al Comune di, ai sensi dell'art. 150, comma 2, del Codice, di provvedere, entro dieci giorni dall'avvenuta ricezione del presente provvedimento, all'oscuramento, all'interno dell'ordinanza indicata nell'atto introduttivo del procedimento e tuttora pubblicata nell'archivio dell'albo pretorio on-line dell'ente resistente, dei dati catastali dell'immobile di proprietà dei ricorrenti, adottando altresì le misure tecniche idonee ad evitare il persistere del collegamento, tramite i motori di ricerca generalisti, tra il nominativo della ricorrente e la pagina del sito contenente le ordinanze del settore edilizio;

Sanzione: condanna alle spese del procedimento pari a euro 500,00 di cui 250,00 devono essere versati al ricorrente.

Parere Garante: n. 278 del 09/05/2018

Fattispecie: relativo a una richiesta di riesame sul provvedimento di diniego di un accesso civico.

Nello specifico, oggetto dell'accesso civico risulta essere «**l'attestazione del conseguimento della laurea in Giurisprudenza con indicazione della data della seduta pubblica di laurea** sostenuta dall'allora studentessa [identificata in atti]».

L'Università ha riscontrato la predetta richiesta di accesso civico, rappresentando che «il dato richiesto non rientra tra i documenti pubblici per i quali è previsto l'accesso civico generalizzato. Tale istituto è stato infatti creato principalmente allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dal co. 2 lett. c) dell'articolo 5-bis del D. Lgs 33/2013». L'amministrazione ha, al riguardo, precisato che «l'intera carriera dello studente è tutelata dal D. lgs. 196/2003 e dai relativi regolamenti».

Nella richiesta di riesame il soggetto istante si è opposto al predetto diniego richiedendo nello specifico la «copia o attestazione del diploma di laurea in Giurisprudenza a nome [del soggetto identificato in atti], ove conseguito, rammentandosi che [il predetto soggetto] non è più, laddove abbia conseguito la laurea, nello status di studente».

Contenuto del parere: l'accesso civico è "rifiutato", fra l'altro, «se il diniego è necessario per evitare un pregiudizio concreto alla tutela [della] protezione dei dati personali, in conformità con la disciplina legislativa in materia» (art. 5-bis, comma 2, lett. a)) e che va comunque "escluso", oltre che nei casi di segreto di Stato, e nei casi di divieti di accesso o divulgazione previsti dalla legge, anche nei «casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della legge n. 241 del 1990».

il rilascio di certificati da parte delle Università – come quello relativo al conseguimento della laurea – è disciplinato dalla specifica normativa di settore, contenuta nel d.P.R. n. 445 del 28/12/2000.

.... agli uffici pubblici è vietato rilasciare, persino al soggetto interessato, certificati da esibire ad altre pubbliche

amministrazioni e ai gestori di pubblici servizi (art. 40 del d.P.R. n. 445/2000) e che **le certificazioni rilasciate dalla pubblica amministrazione in ordine a stati, qualità personali e fatti sono valide ed utilizzabili solo nei rapporti tra privati.**

Per il rilascio di ciascun certificato è previsto, in ogni caso, il pagamento dell'imposta di bollo e dei diritti di segreteria ai sensi del d.P.R. 26/10/1972, n. 642, a esclusione degli usi ivi indicati.

Nei rapporti con gli organi della pubblica amministrazione e i gestori di pubblici servizi, i certificati e gli atti di notorietà sono sempre sostituiti dalle dichiarazioni sostitutive. Le amministrazioni pubbliche e i gestori di pubblici servizi «sono tenuti ad acquisire d'ufficio le informazioni oggetto delle dichiarazioni sostitutive di cui agli articoli 46 e 47, nonché tutti i dati e i documenti che siano in possesso delle pubbliche amministrazioni, previa indicazione, da parte dell'interessato, degli elementi indispensabili per il reperimento delle informazioni o dei dati richiesti, ovvero ad accettare la dichiarazione sostitutiva prodotta dall'interessato» (art. 43, comma 1, del d.P.R. n. 445/2000).

Il rilascio del certificato di laurea pertanto è sottoposto a specifiche regole che non possono essere superate tramite la disciplina sull'accesso civico, né se a richiedere il medesimo certificato sia il soggetto interessato, né tantomeno se sia un soggetto terzo estraneo.

La citata disciplina di settore contenuta nel d.P.R. n. 445/2000 non è quindi derogabile dalle disposizioni contenute nel d. lgs. n. 33/2013, che peraltro prevedono espressamente che l'accesso civico debba essere «escluso» nei casi in cui «l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti [...]».

In conformità con i precedenti orientamenti del Garante (Parere n. 459 del 9/11/2017, in www.gdpd.it, doc. web n. 7156608; Parere n. 434 del 26/10/2017, doc. web n. 7156279), l'esclusione dei predetti documenti dall'accesso documentale ai sensi della l. n. 241/1990, comporta l'esclusione su di essi anche dell'accesso civico (cfr. TAR Lazio, sez. 1, 3/7/2017 n. 7592; vd. anche TAR Veneto 10/5/2017 n. 463. Sul punto vd. anche Consiglio di Stato, sez. IV, 13/7/2017 n. 3461 che, con riferimento all'accesso civico disciplinato dall'art. 5, commi 1 e 2 del d. lgs. n. 33/2013, ha precisato che «Come la giurisprudenza ha già avuto modo di affermare (Cons. Stato, sez. VI, 20 novembre 2013 n. 5515), l'accesso civico disciplina situazioni non ampliative, né sovrapponibili a quelle che consentono l'accesso ai documenti amministrativi, ai sensi degli artt. 22 ss. l. n. 241/1990». Cfr. anche TAR Veneto n. 463/2017, cit., laddove si afferma che «In sostanza, l'accesso civico non può essere utilizzato per superare, in particolare in materia di interessi personali e dei principi della riservatezza, i limiti imposti dalla legge 241 del 1990»).

l'Università, seppur con una sintetica motivazione, abbia correttamente respinto l'accesso civico alla documentazione richiesta.

Provvedimento Garante: n. 292 del 16/05/2018

Fattispecie: **determinazione con cui si stabilisce che un dipendente comunale debba astenersi per conflitto di interessi riguardo alla valutazione di altra dipendente comunale a cui è legato da rapporto di coniugio, pubblicata, per oltre tre anni oltre il termine di 15 giorni prescritti, nell'Albo pretorio online e reperibile anche nella sezione "Amministrazione trasparente", contenente dati personali del segnalante e della moglie, quali, oltre i dati identificativi dei coniugi, informazioni sull'esistenza di un rapporto di lavoro presso l'ente e di un potenziale conflitto di interessi nell'anno XX.**

La pubblicazione facoltativa di tale determina è prescritta dall'art. ... dello Statuto comunale.

Violazioni: Siccome la deliberazione della Giunta con cui è stato stabilito di pubblicare tutte le determinazioni è definito "atto di indirizzo" non ha come contenuto un regolamento;

Il Garante rilevata l'illiceità del trattamento dei dati effettuato dal Comune di XX nei termini indicati in premessa:

- 1) vieta, ai sensi dei citati artt. 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice, al Comune di XX l'ulteriore diffusione – sia attraverso la pubblicazione nell'area dedicata all'Albo Pretorio online, che in qualsiasi altra parte del sito web istituzionale – dei dati personali contenuti nella Determinazione del Settore Ufficio del Segretario Generale n. XX del XX avente a oggetto «XX» ([url http://...](http://...));
- 2) prescrive per il futuro, ai sensi degli artt. 143, comma 1, lett. b), e 154, comma 1, lett. c), del Codice, al Comune di XX di adottare gli opportuni accorgimenti affinché le modalità di pubblicazione delle deliberazioni contenenti dati personali sul sito web istituzionale e, in particolare, sull'albo pretorio online rispettino le indicazioni – relative al mantenimento della diffusione dei dati in Internet per il tempo previsto dalla disciplina di settore – fornite dal Garante nella parte seconda, par. 3.a, del citato Provvedimento n. 243 del 15 maggio 2014, recante le «Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati»;

Sanzione: Il Garante si è riservato di attivare il procedimento sanzionatorio.

Provvedimento Garante: n. 209 del 07/11/2019

Fattispecie: deliberazione G.M. contenente dati giudiziari eccedenti e non pertinenti rispetto alla finalità della pubblicazione, pubblicata nell'Albo pretorio online.

Violazioni: il Garante nel provvedimento n. 243 del 15 maggio 2014 ha peraltro evidenziato che, anche in presenza di un obbligo di pubblicazione, i soggetti chiamati a darvi attuazione non possono comunque diffondere i dati personali eccedenti o non pertinenti (cfr. parte seconda parr. 1 e 3.a.). Nello stesso provvedimento è precisato che «fin dalla fase di redazione degli atti e dei documenti oggetto di pubblicazione, nel rispetto del principio di adeguata motivazione, non dovrebbero essere inseriti dati personali "eccedenti", "non pertinenti", "non indispensabili" (e, tantomeno, "vietati"). In caso contrario, occorre provvedere, comunque, al relativo oscuramento» (cfr. parte seconda par. 1). È, inoltre, previsto che «una volta trascorso il periodo di pubblicazione previsto dalle singole discipline di riferimento [es.: art. 124 del d. lgs. n. 267/2000] se gli enti locali vogliono continuare a mantenere nel proprio sito web istituzionale gli atti e i documenti pubblicati, ad esempio nelle sezioni dedicate agli archivi degli atti e/o della normativa dell'ente, devono apportare gli opportuni accorgimenti per la tutela dei dati personali. In tali casi, quindi, è necessario provvedere a oscurare nella documentazione pubblicata i dati e le informazioni idonei a identificare, anche in maniera indiretta, i soggetti interessati» (ivi, par. 3.a); Violazioni accertate:

- 1) mancato rispetto dei principi di "liceità" e "minimizzazione" del trattamento, in violazione dell'art. 5, par. 1, lett. a) e c), del RGPD;
- 2) assenza di un idoneo presupposto normativo, per il periodo eccedente i tempi di pubblicazione previsti dall'art. 124, comma 1, del d. lgs. 267/2000, in violazione dell'art. 19, comma 3, del Codice (vigente all'epoca dei fatti) e dell'art. 6, par. 1, lett. c) ed e); par. 2 e par. 3, lett. b), del RGPD;

Sanzione: euro 6.000,00

Provvedimento Garante: n. 3 del 15/01/2020

Fattispecie: Determinazione, pubblicata nell'Albo pretorio online per oltre due mesi, con cui veniva disposta la liquidazione delle spese legali per un procedimento giudiziario in cui era stato parte il Comune di e nella parte motiva risultavano riportati anche dati e informazioni personali del reclamante, con dettagliati riferimenti alle relative infermità per cause di servizio, come l'indicazione che lo stesso aveva «diritto all'equo indennizzo per XX». Nella stessa deliberazione, inoltre, risultavano riportati anche le coordinate IBAN dell'avvocato incaricato dall'Ente.

Violazioni accertate: si rileva l'illiceità del trattamento di dati personali per avere diffuso :

- dati sulla salute del Sig. XX, con dettagliati riferimenti alle relative infermità per cause di servizio, in violazione dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. c); 9, parr. 1, 2 e 4, del RGPD, nonché dell'art. 2-septies, comma 8, del Codice;
- dati personali non «limitati a quanto necessario rispetto alle finalità» del trattamento, con riferimento alla indicazione in chiaro delle coordinate IBAN dell'avvocato incaricato dall'Ente, in violazione dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. c, del RGPD.

Sanzione: euro 10.000,00

Provvedimento Garante: n. 52 del 05/03/2020

Fattispecie: sul sito web istituzionale del Comune, nella sezione Albo pretorio storico nonché nella sezione denominata «XX», era possibile visualizzare liberamente **la determinazione del responsabile di settore avente a oggetto «XX dinanzi al Tribunale di incarico per la difesa dell'Ente all'avv. ... - impegno di spesa»** – e **il relativo allegato contenente l'atto di citazione del reclamante dinanzi al Tribunale**; i predetti documenti (determinazione e relativo allegato contenente l'atto di citazione) riportavano in chiaro dati e informazioni personali del reclamante nell'oggetto e nel corpo del testo, quali i dati e le informazioni relativi al nominativo del reclamante e alla circostanza che lo stesso ha citato il Comune per risarcimento di danni (patrimoniali e non). Nell'atto di citazione sono riportati i dati e informazioni personali del reclamante quali, oltre il nominativo, la data e il luogo di nascita, la residenza e il codice fiscale, una dettagliata ricostruzione – ai fini dell'instaurazione della causa contro il Comune – di vicende personali, professionali, giudiziarie, nonché di attività politico-amministrativa svolta quando rivestiva la carica di XX.

Violazioni accertate: ... alla luce della delibera n. XX del XX dell'Autorità Nazionale Anticorruzione (ANAC) con la quale sono state approvate le «Linee guida n. 12. Affidamento dei servizi legali», si ritiene infatti di accogliere le osservazioni presentate nelle memorie difensive del Comune, in base alle quali – ai sensi del combinato disposto dell'art. 37 del d. lgs. n. 33/2013 e dell'art. 29 del d. lgs. 50/2016 – deve essere pubblicata sul sito web istituzionale la delibera di affidamento dell'incarico al legale rappresentate per la difesa dell'Ente nei casi ivi previsti.

Ciò tuttavia non legittima affatto il Comune a pubblicare anche l'atto di citazione, come avvenuto nel caso di specie, né a diffondere il nominativo del reclamante (controparte del Comune) riportato nella deliberazione pubblicata, che non risulta necessario rispetto alle finalità del trattamento – ossia l'affidamento di un incarico a un legale del

Comune per la difesa in giudizio – nel rispetto del principio di «minimizzazione» dei dati (art. 5, par. 1, lett. c, del RGPD). Con riferimento a quest'ultimo profilo, infatti, allo scopo di affidare l'incarico al legale era ben possibile identificare la causa attraverso l'indicazione del solo numero di ruolo, senza riportare il nominativo del reclamante oppure pubblicare la delibera provvedendo all'oscuramento del nominativo del reclamante o alla relativa sostituzione con degli omissis.

È, quindi, consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principio di pertinenza e non eccedenza" di cui all'art. 11, comma 1, lett. d, del Codice [oggi "principio di minimizzazione" ai sensi dell'art. 5, par. 1, lett.c), del RGPD]). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti.

Il Comune di risulta aver violato gli artt. 5, par. 1, lett. c; e 6, par. 1, lett. c) ed e); par. 2 e par. 3, lett. b), del RGPD, nonché l'art. 19, comma 3, del Codice vigente al momento dell'inizio della condotta illecita.

Sanzione: euro 3.000

Provvedimento Garante: n. 68 del 25/02/2021

Fattispecie: pubblicazione nell'Albo pretorio online del Comune di di una **determinazione avente ad oggetto la "presa d'atto e accettazione dimissioni volontarie del dipendente dott. [iniziali del cognome e del nome reclamante]" e contenente informazioni relative al rapporto di lavoro al tempo in essere tra il Comune e il reclamante – che era impiegato in qualità di XX presso il Comune –, incluse valutazioni in merito al suo operato e informazioni attinenti al suo stato di salute.**

L'interessato ha, altresì, lamentato la circostanza che tali vicende e valutazioni fossero state menzionate in un articolo del quotidiano XX del XX. Tale articolo riportava, in particolare, alcuni passaggi della determinazione sopra menzionata, nonché una dichiarazione del sindaco del Comune in merito alla circostanza che il reclamante avesse chiesto di beneficiare di un orario di lavoro flessibile e che si fosse assentato dal servizio per malattia durante le festività natalizie.

Violazioni accertate: La disciplina di protezione dei dati personali prevede che i soggetti pubblici, anche qualora operino nello svolgimento dei propri compiti di datori di lavoro, possono trattare i dati personali dei lavoratori, anche relativi a categorie particolari di dati - tra i quali sono ricompresi anche i "dati relativi alla salute" (cfr. art. 9, par. 1, del Regolamento) - se il trattamento è necessario, in generale, per la gestione del rapporto di lavoro e per adempiere a specifici obblighi o compiti previsti dalle norme nazionali di settore (artt. 6, par. 1, lett. c) ed e); 9, par. 2, lett. b) e par. 4; 88 del Regolamento).

La "diffusione" di dati personali (come la pubblicazione online), da parte di soggetti pubblici, è ammessa solo quando prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-ter, commi 1, 3 e 4, lett. b), del Codice).

In ogni caso, i "dati relativi alla salute", ossia quelli "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" (art. 4, par. 1, n. 15, del Regolamento) "non possono essere diffusi" (art. 2-septies, comma 8, del Codice e art. 9, par. 4, del Regolamento).

Sebbene la determinazione in questione non menzionasse espressamente il nome e il cognome del reclamante, quest'ultimo era in ogni caso identificabile attraverso il riferimento alle proprie iniziali. Peraltro, considerato che al tempo il reclamante era XX in servizio presso il Comune e che la determinazione fa riferimento a "[iniziali del cognome e del nome] quale XX", il reclamante risulta essere, in ogni caso, facilmente identificabile, sia all'interno che all'esterno dell'Ente, dovendosi, pertanto, considerare le informazioni contenute nella determinazione, relative al reclamante, come "dati personali" ai sensi dell'art. 4, par. 1, n. 1, del Regolamento (cfr., sul punto, provv.ti 2 luglio 2020, n. 118, doc. web n. [9440025](#), e 2 luglio 2020, n. 119, doc. web n. [9440042](#)).

Per quanto attiene alla circostanza che la determinazione in questione menzionasse solo l'assenza per malattia del reclamante, senza l'indicazione della diagnosi, si rileva che, secondo il costante orientamento del Garante, nella nozione di dato personale relativo alla salute "può rientrare anche una informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla circostanza che sia contestualmente indicata esplicitamente la diagnosi" (par. 8 delle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" del Garante, provv. n. 23 del 14 giugno 2007, doc. web n. [1417809](#); v. anche, con specifico riguardo al contesto lavorativo, provv. 7 maggio 2015, n. 269, doc. web n. [4167648](#); provv. 10 ottobre 2013, doc. web n. [2753605](#); provv.ti 7 luglio 2004, doc. web n. [1068839](#) e [1068917](#); in giurisprudenza, cfr. punto 50 della sentenza della Corte di giustizia delle Comunità europee 6 novembre 2003 C-101/01, Lindqvist, e Cass. civ. Sez. I, 8 agosto 2013, n. 18980, ove si afferma che "non può essere messo in dubbio che un'assenza dal lavoro "per malattia" costituisca un dato personale "relativo alla salute" del soggetto cui l'informazione si riferisce").

In merito a quanto dichiarato dal Comune, ovvero che "con riferimento alla pubblicazione [della determinazione]

sul sito internet del Comune, nella sezione Albo Pretorio, tale adempimento è prescritto ai fini dell'acquisizione dell'esecutività delle singole determinazioni (provvedimenti dirigenziali)", si evidenzia che il Comune non ha comprovato l'esistenza di una specifica norma di legge che stabilisca la pubblicazione di una determinazione di presa d'atto delle dimissioni di un dipendente come requisito ai fini dell'integrazione dell'efficacia dell'atto. Peraltro, anche in presenza di una norma di legge che preveda la pubblicazione di atti e documenti della pubblica amministrazione (cfr. art. 124 del d.lgs. 18 agosto 2000, n. 267) – che in ogni caso deve essere rispettata anche con riguardo all'arco temporale di pubblicazione da questa stabilito - devono essere, comunque, rispettati i principi di protezione dei dati, tra i quali il principio di "minimizzazione dei dati" (art. 5, par. 1, lett. c), del Regolamento; cfr. parte II, par. 3(a), delle Linee guida del Garante sopra citate), fermo restando che, in ogni caso, i dati relativi alla salute non possono essere diffusi (art. 2-septies, par. 8, del Codice).

Nel caso di specie, la determinazione in questione, che riportava informazioni di dettaglio relative a vicende connesse al rapporto di lavoro, nonché valutazioni in merito al suo operato e riferimenti espliciti al suo stato di salute, è stata, peraltro, pubblicata per un periodo molto lungo, circostanza che connota ulteriormente di illiceità la diffusione dei dati personali in essa contenuti.

Premesso che il Comune non aveva alcun obbligo di pubblicare la determinazione in questione, non ricorrendo alcuno dei casi previsti dall'art. 23 del d.lgs. 14 marzo 2013, n. 33 (che, peraltro, prevede la pubblicazione dei soli "elenchi dei provvedimenti adottati"), si rileva che "le pubbliche amministrazioni possono disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti che non hanno l'obbligo di pubblicare ai sensi del presente decreto o sulla base di specifica previsione di legge o regolamento, nel rispetto dei limiti indicati dall'articolo 5-bis, procedendo alla indicazione in forma anonima dei dati personali eventualmente presenti". Il Comune ha, invece, pubblicato la determinazione in questione, peraltro diffondendo dati personali relativi allo stato di salute, in violazione dello specifico divieto previsto dall'art. 2-septies, comma 8, del Codice.

Né rileva quanto affermato dal Comune in merito alla circostanza che la pubblicazione della determinazione in questione sia stata posta in essere in ragione della generica esigenza, rappresentata dal Comune, di difendere il proprio operato nei confronti della collettività e garantire la trasparenza delle proprie scelte, essendo il trattamento – per quanto sopra detto – privo di un'idonea base giuridica.

Parimenti, risultano ingiustificate e illecite le dichiarazioni rese alla stampa (v. definizione di "comunicazione" di cui all'art. 2-ter, comma 4, lett. a) del Codice), ad opera del Comune, nella persona del Sindaco, con riguardo ad informazioni relative al rapporto di lavoro, inclusi i dati relativi allo stato di salute dell'interessato, in assenza di un'idonea base giuridica e in violazione dell'art. 2-septies del Codice, con conseguente ulteriore diffusione a mezzo stampa dei medesimi dati.

Alla luce delle considerazioni che precedono, il complessivo trattamento risulta essere avvenuto in violazione degli artt. 5, par. 1, lett. a) e c), 6 e 9 del Regolamento e degli artt. 2-ter e 2-septies, comma 8, del Codice.

Sanzione: euro 6.000,00

Provvedimento Garante: n. 107 del 25/03/2021

Fattispecie: pubblicata all'Albo pretorio online una **determina con cui si stabiliva di «autorizzare lo svincolo del bonifico bancario effettuato dai Sigg. XX e XX in nome e per conto della XX, presso il Banco di Napoli in data XX, a favore del Comune di di € XX».** La citata determinazione conteneva i nominativi dei soggetti interessati e il codice iban del conto corrente – a loro cointestato – su cui effettuare il versamento.

Alla predetta determinazione risultavano allegate: a) la nota del Comune prot. n. XX del XX, indirizzata all'XX, con la quale si chiedeva al presidente dell'associazione XX l'autorizzazione allo svincolo del bonifico bancario effettuato dai Sigg. XX e XX, contenente i medesimi dati personali prima descritti; b) la nota prot. n. XX del XX, indirizzata al Comune, contenente la dichiarazione rilasciata dal presidente della predetta associazione XX (odierno reclamante) con i relativi dati personali (quali, oltre al nominativo, la data e il luogo di nascita, la residenza e la copia fronte retro della carta d'identità).

I predetti documenti erano scaricabili.

Violazioni accertate: Il Garante concorda con il Comune per quanto concerne la non applicazione del RGPD alle persone giuridiche, enti o associazioni e ai relativi dati di contatto (es: nome e indirizzo della sede dell'XX, eventuale numero di telefono, ecc.) anche se coincidono con i dati del legale rappresentante, mentre costituisce violazione del RGPD la diffusione di quei "dati personali", in alcuni casi sicuramente non necessari, dei soggetti che agivano in nome e per conto dell'Associazione, quali nominativi e codice iban, nonché — nel caso del reclamante — data e luogo di nascita, residenza e persino, la copia integrale della carta d'identità.

Il Garante ritiene che ogni eventuale utilizzo illecito di tali dati (quale ad esempio un furto di identità) riverbererebbe i propri effetti negativi nella sfera giuridica delle persone fisiche a cui si riferiscono e non necessariamente in quella dell'associazione.

Le pubblicazioni all'Albo pretorio, a cui non si applicano le disposizioni del d.lgs. n. 33/2013, devono essere rimosse una volta decorso il termine dei 15 giorni previsti dal TUEL.

In conformità al principio di minimizzazione dei dati previsto dall'art. 5, par. 1, lett. c), del RGPD, il titolare del

trattamento è obbligato a svolgere in ogni caso un'analisi volta a valutare se i dati personali oggetto di pubblicazione siano effettivamente «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, par. 1, lett. c, del RGPD).

Sanzione: euro 4.000,00

ARCHIVIO ONLINE

Provvedimento Garante : n. 556 del 21/12/2017

Fattispecie : **Determinazione dirigenziale contenente dati e informazioni personali di terzi, pubblicata nella sezione archivio sul sito web istituzionale**

Violazioni : illecita diffusione oltre il termine di pubblicazione prescritto dall'art. 124, c. 1., d.lgs. 267/2000 e dell'art. 19, c. 3, del Codice; se gli enti locali vogliono continuare a mantenere nel proprio sito web istituzionale gli atti e i documenti pubblicati, ad esempio nelle sezioni dedicate agli archivi degli atti e/o della normativa dell'ente, devono oscurare nella documentazione pubblicata i dati e le informazioni idonei a identificare, anche in maniera indiretta, i soggetti interessati.

Sanzione: euro 20.000,00

Provvedimento Garante: n. 324 del 16/09/2021

Fattispecie: sul sito web istituzionale del Comune nell'area «Documenti e dati»/«Albo pretorio»/«storico» era possibile visualizzare e scaricare liberamente la **determinazione di liquidazione di un contribuente, che riportava in chiaro, nel testo e nell'oggetto, dati e informazioni personali, quali il nominativo del reclamante e del padre a suo carico con indicazione della relativa situazione di disabilità in quanto portatore di handicap.** Nel testo della delibera erano inoltre contenuti la data e il luogo di nascita, la residenza, nonché le informazioni relative alla liquidazione dell'importo del contributo previsto per il superamento e l'eliminazione di barriere architettoniche presenti nel proprio alloggio con indicazione dell'indirizzo del soggetto disabile, dei singoli lavori effettuati (compresi i riferimenti dettagliati alle fatture e l'indicazione dell'impresa di lavori a cui ci si è rivolti).

Violazioni accertate: rileva l'illiceità del trattamento di dati personali effettuato dal Comune di, in quanto:

- 1) la diffusione dei dati sulla salute del genitore del reclamante, è avvenuta in violazione del divieto previsto dall'art. 2-septies, comma 8, del Codice e dall'art. 9, par. 1, 2 e 4, del RGPD;
- 2) la diffusione dei dati e delle informazioni personali — quali la data e il luogo di nascita, la residenza, le informazioni relative alla liquidazione dell'importo del contributo previsto per il superamento e l'eliminazione di barriere architettoniche presenti nell'alloggio con indicazione dell'indirizzo del soggetto disabile, i singoli lavori effettuati (comprese le fatture e l'indicazione dell'impresa di lavori a cui ci si è rivolti) — è avvenuta in violazione del principio di «minimizzazione» dei dati, considerando che gli stessi non risultano essere stati «limitati a quanto necessario rispetto alle finalità per le quali sono trattati», di cui all'art. 5, par. 1, lett.c), del RGPD;
- 3) la diffusione dei dati del reclamante è avvenuta in assenza di idonei presupposti normativi per il periodo eccedente i quindici giorni previsti dall'art. 124, comma 1, del d. lgs. n. 267/2000 per la pubblicazione nell'albo pretorio, in violazione dell'art. 2-ter, commi 1 e 3, del Codice; nonché dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD.

Sanzione: euro 5.000,00

ATTI GIUDIZIALI

Provvedimento Garante : n. 169 del 29/04/2021

Fattispecie : visionabile e scaricabile **delibera della Giunta Comunale per opposizione ad atto di citazione di precetto, pubblicato nella sezione Amministrazione Trasparente e nell'Albo pretorio online.**

Violazioni : diffusione di dati e informazioni personali del reclamante (quali nominativo; riferimenti particolareggiati relativi ad atti di precetto, e relativa opposizione, per pagamenti nei confronti del Comune a seguito dell'avvio di procedimento esecutivo immobiliare) in violazione del principio di minimizzazione dei dati ex art. 5, par. 1, lett. c) RGPD. La diffusione risulta priva di idonei presupposti normativi per il periodo eccedente i quindici giorni previsti dall'art. 124, comma 1, del d. lgs. n. 267/2000 per la pubblicazione nell'albo pretorio, in violazione dell'art. 2-ter, commi 1 e 3, del Codice; nonché in violazione dei principi di base del trattamento contenuti negli artt. 5, par. 1,

lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD.

La pubblicazione nella sezione "delibere" per la finalità trasparenza "non prevede la diffusione del documento ma solo di informazioni per estratto degli stessi".

Sanzione in euro : 2.000,00

Provvedimento Garante : n. 3 del 15/01/2020

Fattispecie : Determina di **liquidazione spese legali per procedimento giudiziario** pubblicata all'Albo pretorio online

Violazioni : illecita diffusione di dati sensibili con dettagliati riferimenti alle relative infermità per cause di servizio di una dipendente-reclamante come l'indicazione che lo stesso aveva «diritto all'equo indennizzo» e, inoltre, risultavano riportati anche le coordinate IBAN dell'avvocato incaricato dall'Ente, in violazione dell'art. 2-septies, c. 8, del Codice, e anche dell'art. 9, prf.. 1, 2 e 4, del RGPD;
violazione del principio di minimizzazione dei dati ex art. 5, prf.1, lett. c) RGPD

Sanzione in euro 10.000,00

Provvedimento Garante n. 274 del 17/12/2020

Fattispecie : **determinazione**, pubblicata sul sito istituzionale e nella sezione Amministrazione Trasparente, contenente dati e informazioni personali del reclamante, fra cui oltre il nome e cognome, il riconoscimento della liquidazione delle spese di lite, e l'indicazione del codice IBAN del conto corrente dello stesso;

Violazioni : violazione degli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD; nonché l'art. 2-ter, commi 1 e 3 del Codice; assenza di fondamento normativo;

Sanzione: euro 4.000,00

Provvedimento Garante n. 272 del 17/12/2020

Fattispecie: **delibera GM**, pubblicata nella sezione Amministrazione Trasparente e all'Albo pretorio, **contenente una denuncia-querela da parte del Sindaco nei confronti di un consigliere comunale.**

Violazioni :

- illecita diffusione dei dati oltre il termine prescritto ex art. 124, c. 1, TUEL, in violazione dell'art. 19 comma 3 del Codice
- principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD

Sanzione: euro 10.000,00

BUSTA PAGA

Provvedimento Garante: n. 1063659 del 19 febbraio 2002

Fattispecie: Il ricorrente lamenta che nei cedolini mensili del proprio stipendio è apposta la dicitura "pignoramento" che attualmente descrive in dettaglio due detrazioni ritenute dal ricorrente medesimo adeguatamente individuabili in base al solo codice n. 543 apposto a margine della somma detratta.

Il ricorso è fondato solo parzialmente.

Violazioni accertate: Il trattamento dei dati idonei a rivelare la finalità della ritenuta nel cedolino è, in termini generali, lecito e correlato alle finalità del trattamento, che è volto anzitutto a documentare al lavoratore le diverse voci relative alle competenze e alle trattenute anche per permettere una verifica agevole circa l'esatta corresponsione della retribuzione.

Tale finalità di documentazione e di trasparenza, laddove vengano in considerazione specifiche voci che rivelano delicati aspetti relativi a peculiari rapporti familiari o a determinati provvedimenti giudiziari, possono essere ugualmente perseguite, nel rispetto del principio di pertinenza e non eccedenza delle informazioni trattate (art. 9, comma 1, lett. d), legge n. 675/1996), mediante l'utilizzo di diciture meno specifiche che rendano ugualmente comprensibile la voce (a puro titolo di esempio: "altre trattenute"), oppure di idonei codici identificativi (come quello apposto a margine nel caso di specie), tenendo peraltro presente che tali indicazioni possono essere peraltro oggetto di eventuali richieste di chiarimenti rivolte dal lavoratore agli uffici amministrativi dell'ente.

Tali cautele, pur riguardando un documento certamente relativo al rapporto tra datore di lavoro e dipendente, evitano che, in caso di richiesta di esibizione o di produzione del cedolino da parte di soggetti ai quali l'interessato abbia ad esempio richiesto un finanziamento, divengano chiaramente conoscibili a terzi delicati aspetti relativi alla sfera privata del lavoratore, oppure notizie eccedenti la finalità perseguita con il cedolino (si pensi, oltre che

<p>alla specifica causale del pignoramento, alla superflua indicazione della sigla identificativa del sindacato destinatario della ritenuta sindacale).</p> <p>Il cedolino dello stipendio può essere esibito o prodotto in circostanze nelle quali interessa appurare unicamente il livello stipendiale e non anche tutte le causali delle varie voci, in particolare di quella in esame.</p> <p>In altri casi, invece, <u>il cedolino (o altro documento che lo sostituisca rilasciato dal datore di lavoro) viene richiesto da terzi anche per identificare la porzione di retribuzione "disponibile" a garanzia del credito, in particolare per mutui e finanziamenti conseguenti anche a c.d. cessioni del quinto dello stipendio</u>. In questi casi, fermo restando quanto sopra indicato circa la necessità di evitare l'indicazione della specifica causale (es.: alimenti al coniuge), <u>la cautela da adottare deve tuttavia permettere di individuare la predetta parte di retribuzione</u>.</p> <p><u>Solo entro questi limiti, quindi, l'ente dovrà provvedere a modificare la dicitura "pignoramento" utilizzando una diversa dizione o codice, o utilizzando altra espressione che renda enucleabile la ritenuta senza descriverla specificamente, oppure articolando diversamente la parte del cedolino relativo alle detrazioni nei termini appena indicati (avvalendosi anche, in caso di difficoltà di esecuzione del presente provvedimento, del procedimento dinanzi al Garante di cui all'art. 20, comma 11, del citato d.P.R. n. 501/1998).</u></p>
<p>Sanzione: euro</p>

CONCORSI PER ASSUNZIONI

<p>Provvedimento Garante n. 86 del 12/02/2015</p>
<p>Fattispecie: diffusione di dati personali, contenuti nella documentazione relativa agli esiti delle prove intermedie sostenute dai partecipanti a un concorso pubblico indetto dal Comune e risalente al 2008, sul sito del Comune <u>in assenza di una norma legislativa o regolamentare</u> che quella pubblicazione autorizzasse.</p>
<p>Violazioni: la previsione contenuta nel bando di concorso riferita al regime di pubblicità delle prove intermedie non soddisfa i requisiti richiesti dall'art. 19, comma 3, del Codice, attesa la <u>natura non regolamentare propria del bando</u>; risulta, inoltre, errato il richiamo agli artt. 23 e 8 del d. lgs. 33/2013 in materia di trasparenza: occorre al riguardo premettere che tale norma, anche ove fosse ritenuta applicabile al caso di specie, essendo stata introdotta solo nel 2013, non potrebbe essere tenuta in considerazione in ossequio al principio del <i>tempus regit actum</i>, secondo il quale, in ambito sanzionatorio, eventuali disposizioni più favorevoli sopravvenute non sanano l'illecito; nel merito deve peraltro osservarsi che la disposizione legislativa richiamata obbliga alla sola pubblicazione, anche in materia di concorsi, del contenuto, oggetto ed eventuale spesa prevista senza, dunque, alcun riferimento agli esiti delle prove espletate; rilevato infine che, destinatario della contestazione, in materia di protezione dei dati personali, può essere anche la persona giuridica titolare del trattamento (art. 4, comma 1, lett f) del Codice) in forza del rapporto di specialità nel quale si pone il Codice rispetto alle norme della legge 689/1981 (art. 166 del Codice);</p>
<p>Sanzione: euro 4.000,00</p>
<p>Provvedimento Garante n. 384 del 06/12/2012</p>
<p>Fattispecie: persistente pubblicazione, sul sito web istituzionale del Comune, di nomi, cognomi ed esiti (espressi in termini numerici) delle prove intermedie (scritta e pratica) sostenute dai partecipanti non ammessi a sostenere la prova orale di un concorso, risalente al 2008, concorso al quale lo stesso reclamante ha partecipato.</p>
<p>Violazioni: la diffusione può essere lecitamente effettuata da parte di un soggetto pubblico unicamente quando tale operazione sia prevista da una norma di legge o di regolamento (art. 2-ter, comma 1, del Codice). Nel caso di specie <u>il trattamento posto in essere risulta illecito atteso che la disciplina di settore contenuta nell'art. 15, comma 6 bis, d.P.R. 9 maggio 1994, n. 487 (Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi) dispone, in primo luogo, che siano pubblicate "nell'albo pretorio del relativo ente" le sole graduatorie definitive dei vincitori di concorso presso gli enti locali territoriali e non anche, come nel caso di specie, gli esiti delle prove intermedie</u>. D'altro canto, la previsione contenuta nel bando di concorso riferita al regime di pubblicità delle prove intermedie, non soddisfa comunque i requisiti richiesti dal menzionato art. 19, comma 3, del Codice, attesa la natura di atto non regolamentare propria del bando. La diffusione risulta altresì illecita per violazione dell'art. 124 del d.lgs. 267/2000 per essere stata protratta oltre il <u>termine di 15 giorni</u>.</p>
<p>Sanzione: euro 4.000,00</p>

Provvedimento Garante n. 154 del 03/09/2020
Fattispecie: pubblicazione nella sezione “Amministrazione trasparente” dei verbali della Commissione giudicatrice e della graduatoria di merito di un concorso per l’assunzione di personale pubblicato nella sezione Amministrazione Trasparente.
Violazioni: <u>illecita diffusione di dati (quali dati identificativi ed esiti delle prove intermedie non superate) dei soggetti concorrenti non vincitori, non ammessi o che si sono ritirati dal concorso, in assenza di idonei presupposti normativi</u> e, dunque, in violazione dell’art. 2-ter, commi 1 e 3, del Codice e dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD (cfr. anche la disposizione contenuta nell’art. 15, comma 6-bis, del d.P.R. 9/5/1994, n. 487)
Sanzione: euro 2.000,00

Provvedimento Garante: n. 106 del 25/03/2021
Fattispecie: è stata lamentata la pubblicazione nella sezione “Amministrazione trasparente” della determina n.XX del XX , da parte del Comune di, avente ad oggetto il “XX”, <u>contenente i dati personali della reclamante e degli altri partecipanti alla procedura concorsuale, tra cui la residenza anagrafica. La delibera, inoltre, era reperibile anche in rete, tramite i motori di ricerca.</u>
Violazioni accertate: Si rileva l’illiceità del trattamento di dati personali effettuato dal Comune di, per aver diffuso dati personali relativi alla reclamante contenuti nella determina n. XX del XX avente ad oggetto il “XX” <u>in assenza di idonei presupposti normativi</u> , in violazione dell’art 6 del Regolamento e dell’art. 2-ter, del Codice, nonché <u>in violazione dei principi di base del trattamento</u> contenuti nell’art. 5, par. 1, lett. a) e c) del Regolamento. <u>Le norme afferenti le procedure di selezione del personale prevedono che siano pubblicate le sole graduatorie definitive dei vincitori di concorso e non anche gli esiti delle prove intermedie o ulteriori dati personali dei concorrenti, tra cui la residenza</u> (cfr. art. 7, d.P.R. 10 gennaio 1957, n. 3; nonché art. 15, d.P.R. 9 maggio 1994, n. 487, in particolare, commi 5, 6 e 6 bis; art. 35, comma 3, d. lgs. 30 marzo 2001, n. 165). <u>Vedasi le Linee guida in materia di trasparenza, anche con riferimento alla pubblicazione delle graduatorie dei concorsi pubblici (provv. n. 243 del 15 maggio 2014, doc. web n. 3134436, spec. II, par. 3.b), ma vedi anche 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, n.161, doc web n.1417809).</u> <u>Il d.lgs. 14 marzo 2013, n. 33, inoltre, non contiene alcuna disposizione che preveda la pubblicazione obbligatoria di tale tipologia di atti o, in generale, di determinazioni che riportino dati personali dei candidati, tra cui il dato relativo alla residenza.</u> <u>Il Comune non avrebbe dovuto indicizzare la pagina del proprio sito web, che ospitava la determina oggetto del reclamo, sui motori di ricerca generalisti, atteso che l’art. 9 del d.lgs. 14 marzo 2013, n. 33, che prevede il divieto per le amministrazioni pubbliche di “disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione Amministrazione trasparente”, non era applicabile al caso di specie.</u>
Sanzione: euro 4.000,00

CONSIGLIERI COMUNALI

Parere Garante: n. 48079 del 14/06/1999
Fattispecie: è stato chiesto di conoscere se un consigliere comunale, per l’espletamento dei compiti connessi con il suo mandato, possa prendere visione dei cedolini degli stipendi di alcuni dirigenti del Comune.
Contenuto parere: <u>necessità di adottare le opportune misure volte a tutelare la riservatezza dei dipendenti per fare in modo che i dati contenuti nel cedolino non siano immediatamente accessibili ad altre persone, rimanendo conoscibili dai soli incaricati del trattamento che li devono necessariamente utilizzare per la gestione del rapporto di lavoro.</u> <u>Nel caso in esame, dunque, il diritto del consigliere comunale di valutare con piena cognizione di causa la correttezza e l’efficacia dell’operato dell’Amministrazione, e di accedere, a tale scopo, ai documenti e a qualsiasi notizia o informazione utili ai fini dell’esercizio delle funzioni consiliari, può essere soddisfatto attraverso altre modalità quali, ad esempio:</u> la pubblicità della situazione patrimoniale dei dirigenti; l’esame dei contratti collettivi, destinati per loro natura ad un regime di diffusa conoscibilità; l’accesso alle deliberazioni e alle determinazioni, riguardanti indennità e altri emolumenti corrisposti, adottate dall’Amministrazione a favore dei dipendenti.

CONTRATTI PUBBLICI

Parere Garante n. 115 del 23/05/2019

Fattispecie: la richiesta di accesso civico riguarda dati, informazioni e documenti contenenti un gran numero di dati personali riferiti a più di 1700 unità, di specie differente, riguardanti, in particolare, **la lista del personale utilizzato nei vari servizi, il curriculum vitae del personale, la documentazione comprovante il possesso dei titoli, competenze ed esperienze previste per le varie figure professionali, la documentazione richiesta per il personale addetto allo specifico servizio identificato in atti e, in ogni caso «Ogni altro atto e/o documento prodotto in fase di partecipazione e di offerta tecnica atto a dimostrare l'idoneità organizzativa tecnica e professionale degli aggiudicatari e del personale impiegato».**

il Ministero ha negato l'accesso civico, evidenziando il coinvolgimento di «una mole consistente di soggettiterzi, aventi immediato e diretto riflesso sull'identità, il domicilio, i recapiti (residenziali e telefonici), sullo stato familiare, attitudini e capacità culturali, professionali e lavorative. L'ostensione dei curricula vitae del personale addetto ai servizi oggetto di gara non può che comportare, pertanto, una immediata e diretta compressione del diritto alla riservatezza dei dati personali, posto che, nella documentazione di cui si chiede l'accesso, sono presenti informazioni sensibili». L'amministrazione ha, inoltre, eccepito il carattere massivo della richiesta di accesso – anche considerando che gli «atti e documenti di cui si chiede l'ostensione sono relativi ai soggetti impiegati nell'espletamento dei servizi in appalto che superano le 1.700 unità» – idoneo a «"paralizzare" per un periodo di tempo significativo l'intero Ufficio con compromissione dei servizi istituzionali».

Violazioni accertate:

premessa: , la fattispecie sottoposta all'attenzione del Garante – come rilevato dalla più recente giurisprudenza amministrativa (cfr. TAR Lazio, Roma, sez. II, 14/01/2019, n. 425; TAR Lombardia, Milano, sez. I, n. 630; TAR Marche, Ancona, sez. I, 18/10/2018, n. 677; TAR Emilia Romagna, Parma, sez. I, 18/07/2018, n. 197; TAR Puglia, Lecce, sez. II, 12/04/2019, n. 599; cfr. anche TAR, Toscana, sez. III, 17/04/2019 N. 577) – ricade in una delle ipotesi di "esclusione" dell'accesso civico generalizzato, considerando che «Il diritto di cui all'articolo 5, comma 2, è escluso nei [...] casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della legge n. 241 del 1990» (art. 5-bis, comma 3, del d. lgs. n. 33/2013).

La giurisprudenza ritiene che «l'accesso agli atti concernenti la procedura di affidamento e la fase di esecuzione dei contratti pubblici è oggetto di una disciplina ad hoc, costituita dalle apposite disposizioni contenute nel Codice dei contratti pubblici e, ove non derogate, da quelle in tema di accesso ordinario recate dalla legge n. 241 del 1990. In tale ambito non trova perciò applicazione l'istituto dell'accesso civico generalizzato, stante la clausola di esclusione contenuta nel richiamato articolo 5- bis, comma 3, del decreto legislativo n. 33 del 2013» (sent. TAR Lazio n. 425/2019, cit.). La scelta del legislatore ... coinvolge interessi privati di natura economica e imprenditoriale di per sé sensibili (e quindi astrattamente riconducibili alla causa di esclusione di cui al comma 2, lett. c), dell'art. 5-bis del d.lgs. n. 33 del 2013), specie quando tali interessi, dopo l'aggiudicazione, vanno a porsi su di un piano pari ordinato – assumendo la connotazione di veri e propri diritti soggettivi - rispetto a quelli della stazione committente" (così ancora TAR Parma, n. 197 del 2018, cit.)» (Ibidem).

Siccome, a differenza dei documenti a cui si è avuto accesso ai sensi della l. n. 241 del 7/8/1990, i dati e i documenti che si ricevono a seguito di una istanza di accesso civico generalizzato divengono «pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7», sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, del d. lgs. n. 33/2013). Anche alla luce di tale amplificato regime di pubblicità dell'accesso civico che va verificata l'esistenza di un possibile pregiudizio concreto alla protezione dei dati personali dei soggetti controinteressati, in base al quale decidere se rifiutare o meno l'accesso civico alle informazioni e ai documenti richiesti. La decisione sulla eventuale ostensione di dati personali nell'ambito del procedimento di accesso civico, deve inoltre tener conto anche nel rispetto dei principi indicati dall'art. 5 del Regolamento (UE) 2016/679 (RGPD), fra cui quello di «minimizzazione dei dati», secondo il quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, par. 1, lett. c), in modo che non si realizzi un'interferenza ingiustificata e sproporzionata nei diritti e libertà delle persone cui si riferiscono tali dati (cfr. anche art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; art. 8 della Carta dei diritti fondamentali dell'Unione europea e della giurisprudenza europea in materia).

decisione: Si tratta di dati e informazioni, attinenti ad aspetti dettagliati della vita lavorativa che, in caso di accoglimento dell'istanza di accessocivico, diverrebbero pubblici e tendenzialmente riutilizzabili (cfr. art. 3, comma 1, del d. lgs. n. 33/2013); ma che, invece, per motivi individuali non sempre si desidera portare a conoscenza di soggetti estranei e consentire peraltro che vengano riutilizzati per altre finalità non conosciute né conoscibili al momento della loro acquisizione da parte del richiedente l'accesso. La relativa ostensione, inoltre, considerando anche la quantità e qualità dei dati personali coinvolti, può avere – in relazione ai casi e al contesto in cui

possono essere utilizzate da parte di terzi estranei che non è dato conoscere a priori – possibili ripercussioni negative sul piano relazionale, personale, sociale dei soggetti controinteressati, sia all'interno che all'esterno dell'ambiente lavorativo (si pensi, ad esempio, a eventuali prospettive di impiego a cui gli interessati potrebbero aspirare in futuro), integrando proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013, alla luce del quale, ai sensi della normativa vigente e delle indicazioni contenute nelle Linee guida dell'ANAC, l'accesso civico va rifiutato (cfr. in senso conforme anche i precedenti orientamenti di questa Autorità in materia di accesso civico ai curriculum alle altre informazioni personali dei dipendenti: parere n. 162 del 30/3/2017, in www.gpdp.it, doc. web n. [6393422](#); n. 29 del 7/2/2019, ivi, doc. web n. [9086520](#); n. 485 del 29/11/2018, ivi, doc. web n. [9065367](#); n. 231 del 18/4/2018, ivi, doc. web n. [8983308](#); n. 421 dell'11/7/2018, ivi, doc. web n. [9037343](#); n. 466 dell'11/10/2018, doc. web n. [9063969](#)).

Le informazioni di dettaglio contenute nella documentazione richiesta, inoltre, impediscono di poter accordare anche un eventuale accesso civico parziale ai sensi dell'art. 5-bis, comma 4, del d. lgs. n. 33/2013; oscurando, ad esempio, i dati identificativi, di contatto e di residenza (nome e cognome, telefono, indirizzo) ivi contenuti. Tale accorgimento, infatti, non elimina la possibilità che i soggetti interessati siano re-identificati da soggetti terzi, anche all'interno dell'amministrazione stessa, tramite gli ulteriori dati di contesto contenuti nella documentazione richiesta.

Riguardo l'interesse personale dell'istante con cui è stato motivato anche la richiesta di accesso documentale, il Garante afferma che "Per questi aspetti, rimane impregiudicata ogni valutazione del Ministero in ordine alla verifica, nel caso in esame, dell'esistenza di un interesse qualificato dell'istante e dei presupposti per l'esercizio del diverso diritto di accesso ai documenti amministrativi ai sensi degli artt. 22 ss. della citata legge n. 241/1990."

Provvedimento Garante: n. 350 del 29/09/2021

Fattispecie: diffusione di dati e informazioni personali contenuti in un file riportante una **tabella con l'elenco dei procuratori di due società identificate in atti e dei loro familiari maggiorenni conviventi (circa un centinaio di soggetti in tutto), pubblicato online dalla Prefettura - Ufficio Territoriale del Governo di nella sezione riservata alla pubblicazione delle white list**, ossia l'elenco a cui devono iscriversi le imprese che intendono operare in settori considerati dalla normativa antimafia particolarmente esposti al pericolo di infiltrazione criminale».

Violazioni accertate: La Prefettura quando ha ricevuto la segnalazione da XX, si è limitata a cancellare il link al file contestato dal sito web della Prefettura, ma non risulta essere intervenuta sull'url appartenente al dominio della Prefettura segnalato dalla società, dal quale il file era di fatto ancora raggiungibile in rete almeno fino alla verifica preliminare effettuata da questa Autorità a XX e che ne consentiva anche la reperibilità tramite i motori di ricerca come Google. E' intervenuta (come fatto solo dopo la contestazione del Garante) risolutivamente sul proprio sistema informatico.

la pubblicazione del file contestato intitolato «XX» sul sito web istituzionale della predetta amministrazione ha comportato una diffusione di dati e informazioni personali:

- a) non conforme al principio di «minimizzazione» dei dati in quanto gli stessi non sono «limitati a quanto necessario rispetto alle finalità per le quali sono trattati», in violazione dell'art. 5, par. 1, lett. c), del RGPD;
- b) priva di idonei presupposti normativi, in violazione dell'art. 2-ter, commi 1 e 3, del Codice; nonché dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD.

Sanzione: euro 11.000,00

CONTRIBUTI - SOVVENZIONI

Provvedimento Garante: n. 213 del 12/04/2018

Fattispecie: sul sito web istituzionale del Comune di è possibile visualizzare e scaricare liberamente la **determinazione dirigenziale avente a oggetto «Approvazione graduatoria provvisoria per esenzione/riduzione pagamento della Tari XX», alla quale sono allegati due elenchi di soggetti aventi diritto a esenzioni o riduzioni della tassa sui rifiuti (Tari) identificate. Le predette graduatorie riportano in chiaro dati e informazioni personali di n. 3447 soggetti interessati, ordinati in base alla situazione economica (il nome e il cognome, la data di nascita, il codice fiscale, l'importo ISEE, il numero dei componenti del nucleo familiare di n. 3269 soggetti interessati con reddito ISEE familiare fino a € 8.000,00, nonché gli stessi personali riferiti a n. 178 soggetti interessati che riportano «invalidità del 100% e con Isee fino ad €10.00,00».**

Violazioni accertate: Rilevata l'illiceità di detta pubblicazione in quanto anche la disciplina statale in materia di trasparenza prevede che «Restano fermi i limiti [...] relativi alla diffusione dei dati idonei a rivelare lo stato di salute [...]» (art. 7-bis, comma 6, del d. lgs. n. 33 del 14/3/2013, recante «Riordino della disciplina riguardante il

<p>diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni»); e, inoltre, prevede che, <u>in ogni caso, «È esclusa la pubblicazione dei dati identificativi delle persone fisiche destinatarie dei provvedimenti di cui al presente articolo, qualora da tali dati sia possibile ricavare informazioni relative»: «allo stato di salute» o «alla situazione di disagio economico-sociale degli interessati»</u> (art. 26, comma 4, del d. lgs. n. 33/2013).</p> <p>Il Garante ha vietato al Comune di di proseguire la pubblicazione dei predetti dati e ha intimato di trovare idonee misure onde evitare che si ripetessero simili condotte illecite.</p> <p>Sanzione: il Garante si è riservato di determinare la sanzione con successivo provvedimento.</p>
--

<p>Provvedimento Garante: n. 23 del 31/01/2019</p> <p>Fattispecie: sul sito web istituzionale del Comune di erano pubblicate, oltre alla graduatoria oggetto della segnalazione, anche le graduatorie contenenti dati e informazioni personali dei soggetti ammessi ed esclusi dall'attribuzione del "contributo all'affitto ad integrazione del canone di locazione" relativa agli anni 2010, 2011 e 2015, nonché le graduatorie per l'assegnazione degli alloggi per soggetti sfrattati e in situazione di disagio economico-sociale con indicazione del nominativo degli interessati; nelle graduatorie relative ai soggetti sfrattati, inoltre, in alcuni casi, era riportata oltre ai nominativi degli interessati, anche la condizione di invalidità al100%.</p> <p>Violazioni accertate: tale pubblicazione è in contrasto con quanto sancito dall'art. 26, comma 4, del d.lgs. 14 marzo 2013 n. 33, che esclude la pubblicazione di dati identificativi di persone fisiche destinatarie di contributi economici, qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute o alla situazione di disagio economico-sociale degli interessati; la predetta condotta illecita è sanzionata dall'art.162, comma 2-bis, del Codice sia con riferimento alla <u>diffusione di dati personali in assenza di idonei presupposti normativi</u> di cui all'art. 19, comma 3, sia con riferimento al divieto di diffusione dei dati idonei a rivelare lo stato di salute di cui all'art. 22, comma 8, del Codice.</p> <p>Sanzione: euro 6.000,00</p>
--

<p>Provvedimento Garante n. 324 del 16/09/2021</p> <p>Fattispecie: Determinazione di liquidazione di un contributo pubblicata nella sezione "Archivio storico" dell'Albo pretorio online.</p> <p>Violazioni accertate:</p> <ul style="list-style-type: none"> ➤ <u>Illecita diffusione di dati</u> (nominativo del reclamante e del padre con indicazione della relativa situazione di disabilità; la data e il luogo di nascita, la residenza, nonché le informazioni relative alla liquidazione dell'importo del contributo previsto per il superamento e l'eliminazione di barriere architettoniche presenti nel proprio alloggio con indicazione dell'indirizzo del soggetto disabile, dei singoli lavori effettuati, compresi i riferimenti dettagliati alle fatture e l'indicazione dell'impresa di lavori a cui ci si è rivolti), in violazione art. 2-septies, c. 8, Codice e art. 9, prf. 1, 2 e 4, RGPD e in violazione del principio di minimizzazione ex art. 5, par. 1, lett. c), del RGPD ➤ <u>assenza di idoneo presupposto per la pubblicazione oltre i 15 giorni prescritti dall'art. 124, c. 1, d.lgs. 267/2000</u> <p>Sanzione: euro 5.000,00</p>

<p>Provvedimento Garante n. 167 del 29/04/2021</p> <p>Fattispecie: nell'area "Sovvenzioni, contributi,ecc." della sezione «Amministrazione trasparente», era possibile visualizzare informazioni di dettaglio relative ad atti di concessione, concernenti il provvedimento con indicazione in chiaro del nominativo del soggetto beneficiario, del codice fiscale, del sussidio ricevuto e del «Titolo/Norma» del pagamento e relativa giustificazione.</p> <p>Violazioni: <u>l'aver pubblicato il nominativo del soggetto interessato e la circostanza che il contributo economico è stato versato in base a «Piani personalizzati di sostegno a favore di persone con handicap grave, ai sensi della Legge 162/98» ha causato una diffusione di dati personali relativi alla sua salute, in violazione dell'art. 2-septies, comma 8, del Codice e dell'art. 26, comma 4, del d. lgs. 33/2013; violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) e c); 9, parr. 1, 2 e 4, del RGPD.</u></p> <p>Sanzione: euro 3.000,00</p>

<p>Provvedimento Garante n. 296 del 26/07/2021</p> <p>Fattispecie: pubblicazione sul sito web istituzionale di un elenco di studenti istanti borse di studio, contenenti dati quali: domanda, nominativo del richiedente, classe dello studente, codice e denominazione della scuola, numero della domanda, dati relativi all'ISEE</p> <p>Violazioni:</p> <ul style="list-style-type: none"> ➤ <u>assenza di idonei presupposti normativi</u>, in violazione dell'art. 2-ter, commi 1 e 3, del Codice e dell'art. 26, comma
--

<p>4, del d. lgs. 33/2013; nonché dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD;</p> <p>➤ <u>per la pubblicazione dei dati relativi all'ISEE violazione del principio di minimizzazione</u> (art. 5, par. 1, lett. c, del RGPD);</p> <p>➤ <u>per la pubblicazione di dati personali di soggetti non ammessi ad alcun beneficio economico, in assenza di idonei presupposti normativi</u>, in violazione dell'art. 2-ter, commi 1 e 3, del Codice, nonché dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD;</p>
<p>Sanzione: euro 200.000,00</p>

CURRICULUM VITAE

<p>Provvedimento Garante: n. 54 del 11/02/2021</p> <p>Fattispecie: nella pagina web intitolata «Elenco Manager» del Ministero per lo Sviluppo Economico erano visibili e liberamente scaricabili dati personali (nominativo, codice fiscale, e-mail) e curriculum vitae integrale (con ulteriori dati personali come, ad esempio, telefono cellulare, istruzione e formazione, dettagliate esperienze professionali, in alcuni casi anche copia del documento di riconoscimento e della tessera sanitaria ecc.) riferiti a più di cinquemila soggetti interessati, inseriti nell'elenco dei «Manager qualificati e delle società di consulenza».</p> <p>Violazioni accertate: L'Ufficio ha contestato al MISE la violazione dell'art. 2-ter, commi 1 e 3, del Codice e dell'art. 6, par. 1, lett. c) ed e); par. 2 e par. 3, lett. b), del RGPD; – che prevede la possibilità, per i soggetti pubblici, di diffondere dati personali solo se tale operazione è prevista «da una norma di legge o, nei casi previsti dalla legge, di regolamento» – in quanto ha ritenuto che la disciplina prevista dagli artt. 3 ss. del Decreto Direttoriale del XX, non potesse costituire un idoneo presupposto normativo per la diffusione di dati personali ai sensi del Codice, tenuto conto che il decreto direttoriale citato non ha natura regolamentare e non è, in ogni caso, in alcun modo richiamato dall'art. 1, commi 228, 230 e 231, della legge n. 145/2018 (che prevedono l'istituzione dell'elenco dei manager). Ciò in quanto, adottando un criterio sostanziale, la natura del decreto direttoriale citato – contrariamente a quanto sostenuto dal MISE – appare riconducibile più alla categoria dell'«atto amministrativo generale» (che a quella del «regolamento», inteso come atto normativo a contenuto generale e astratto). E, inoltre, la pubblicazione dei predetti dati è avvenuta in maniera non conforme al rispetto dei principi di «liceità», «limitazione della finalità» e «minimizzazione dei dati», in violazione dell'art. 5, par. 1, lett. a), b) e c), del RGPD;</p> <p>[nota bene: per effetto delle modifiche apportate dall'art. 9, comma 5 del D.L. 8 ottobre 2021, n. 139, convertito con modificazioni dalla L. 3 dicembre 2021, n. 205, attualmente anche un «atto amministrativo generale» può costituire una valida base giuridica per il trattamento di dati personali.]</p>
<p>Sanzione: euro 75.000,00</p>

DATA BREACH

<p>Provvedimento Garante n. 5 del 15/01/2021</p> <p>per data breach si intende un incidente di sicurezza in cui dati personali, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato)</p> <p>Fattispecie: perdita, per effetto di un furto, di un disk esterno contenenti dati personali quali copie di documenti di riconoscimento, documenti di tipo fiscale (CUD, modelli F24 e 730), buste paga, pratiche di rimborso e un elenco contenente dati analitici riferiti a procedimenti giudiziari; l'hard disk oggetto di sottrazione sarebbe stato «<u>collegato al server installato in una stanza alla quale può accedere qualsiasi dipendente</u>» dell'Ente sanzionato nonché i dipendenti di una società in house dello stesso Ente.</p> <p>Violazioni: violazione del principio di integrità e riservatezza ex art. 5, par. 1, lett. f), del RGPD, secondo cui i dati personali sono «<u>trattati in maniera da garantire un'adeguata sicurezza dei dati personali</u>, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali»</p>
<p>Sanzione: euro 8.000,00</p>

DATI SENSIBILI

Provvedimento Garante n. 3 dell'08/01/2015
Fattispecie: sul sito web intestato della Regione sanzionata – al link situato nella homepage denominato «Area sviluppo» «Determinazioni Dirigenziali» – sono visibili, e liberamente scaricabili, i documenti indicati dal segnalante, e precisamente: il testo integrale nella cui motivazione sono indicati le disabilità per cui è possibile proporre le istanze di contributi e gli allegati A e B della Determinazione contenenti gli elenchi recanti in chiaro i nominativi dei soggetti che hanno presentato domanda per accedere ai contributi erogati a favore di persone disabili.
Violazioni: <u>illecita diffusione di dati idonei a rivelare lo stato di salute degli interessati</u> , in contrasto con il disposto dell'art. 22, comma 8, del Codice; non può ritenersi legittimata tale diffusione per finalità di trasparenza amministrativa, in quanto l'art. 4, comma 6, del d.lgs. n. 33/2013, prevede che <i>“restano fermi i limiti alla diffusione e all'accesso delle informazioni [...] relativi alla diffusione dei dati idonei a rivelare lo stato di salute”</i> e l'art. 26 del medesimo decreto ribadisce il concetto prevedendo espressamente – relativamente agli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici – l'esclusione della pubblicazione di dati dai quali sia possibile ricavare informazioni relative allo stato di salute degli interessati.
Sanzione:

Provvedimento Garante n. 1 del 09/01/2020
Fattispecie: <u>una e-mail contenente una comunicazione mediante un unico messaggio di posta elettronica indirizzato a un numero plurimo di destinatari (16), i cui indirizzi sono stati inseriti nel campo copia conoscenza (c/c), ha, di fatto, senza giustificato motivo e in assenza di qualsivoglia presupposto normativo, rivelato reciprocamente, alle famiglie coinvolte, lo stato di inadempimento dei minori rispetto agli obblighi vaccinali; tale comunicazione di dati sulla salute si sarebbe potuta evitare inserendo gli indirizzi dei destinatari nel campo denominato “copia conoscenza nascosta” (ccn);</u>
Violazioni: <u>assenza di idoneo presupposto giuridico</u> (v. anche art. 2-sexies del Codice) e in violazione dei principi di base del trattamento (artt. 5 e 9 del Regolamento);
Sanzione: soltanto un ammonimento a conformare il trattamento al Regolamento UE

DATI GIUDIZIARI

Provvedimento Garante: n. 118 del 02/07/2020
Fattispecie: pubblicazione nell'Albo pretorio online, nella sezione “Amministrazione trasparente” e nell'Albo storico della determinazione, al cui interno erano menzionati riferimenti a vicende relative al rapporto di lavoro di cui era parte la reclamante. In particolare, la reclamante <u>ha lamentato che la determinazione contenesse riferimenti alla propria persona, essendo identificabile tramite le iniziali del proprio cognome e nome, nonché dati personali relativi a condanne penali e reati.</u> La reclamante era stata assunta dal Comune di a seguito di una procedura di mobilità esterna per la copertura di un solo postoppresso il medesimo Comune e la stessa era stata assegnata in comando presso l'Unione Comunale del, di cui il Comune fa parte. <u>Dopo alcuni anni dall'assunzione, il Comune, a seguito di un'istruttoria avviata dal proprio Ufficio Procedimenti Disciplinari, dalla quale era emerso, ad avviso del Comune, che l'interessata aveva riportato una condanna penale non definitiva e aveva un procedimento penale in corso nel periodo in cui aveva partecipato alla selezione, aveva disposto la sanzione del licenziamento senza preavviso</u> nei confronti dell'interessata, sul presupposto che quest'ultima non avesse i requisiti per partecipare alla procedura di mobilità esterna, il cui bando prevedeva come requisito indispensabile, autocertificato dall'interessata in fase di stipula del contratto di lavoro, l'assenza di condanne penali e procedimenti penali in corso. Di conseguenza, l'Unione, con propria determinazione, aveva disposto l'esclusione dell'interessata dalla procedura selettiva di mobilità esterna e aveva provveduto alla rettifica, in via di autotutela, di due determinazioni del Comune, con le quali erano stati approvati i verbali della procedura.
Violazioni accertate: <u>diffusione di dati personali relativi alla reclamante contenuti nella determinazione, in assenza di idonei presupposti normativi</u> , in violazione degli artt. 6, paragrafo 1, lett. c) ed e), 2 e 3, lett. b), e 2-ter, commi 1 e 3, del Codice, nonché dei principi di base del trattamento contenuti nell'art. 5, par. 1, lett. a) e c) del Regolamento, <u>in quanto l'operazione di diffusione di dati personali (come la pubblicazione su Internet), da parte di soggetti pubblici, è ammessa solo quando prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento</u> (art. 2-ter, commi 1 e 3, del Codice).
Con specifico riguardo <u>il trattamento dei dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza</u>

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), ovvero solo qualora il trattamento sia autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-octies, commi 1 e 5 del Codice).

Il titolare del trattamento è tenuto, inoltre, a rispettare i principi in materia di protezione dei dati, fra i quali quello di "liceità, correttezza e trasparenza" nonché di "minimizzazione", in base ai quali i dati personali devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" e devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. a) e c), del Regolamento).

In particolare, nel rispetto del principio di "minimizzazione dei dati" (art. 5, par. 1, lett. c), del Regolamento), anche in presenza di un obbligo di pubblicazione, i soggetti chiamati a darvi attuazione non possono comunque diffondere i dati personali eccedenti o non pertinenti (cfr. provv. n. 243 del 15 maggio 2014, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, doc. web n. [3134436](#), parte seconda parr. 1 e 3.a.).

In tale quadro, si osserva, in via preliminare, che non rileva quanto dichiarato dall'Ente con riferimento alla circostanza che la reclamante non fosse identificabile. Considerando che "per identificazione non si intende solo la possibilità di recuperare il nome e/o l'indirizzo di una persona, ma anche la potenziale identificabilità mediante individuazione, correlabilità e deduzione" (Gruppo di Lavoro Art. 29, Parere 05/2014 sulle tecniche di anonimizzazione, WP216), la menzione delle iniziali del cognome e del nome della reclamante all'interno della determinazione era, infatti, idonea a consentirne l'identificazione, quantomeno da parte dei dipendenti del Comune e dei familiari o conoscenti della reclamante, anche in considerazione delle dimensioni del Comune (circa 13749 abitanti) e del proprio organico (84 lavoratori a tempo indeterminato ...

Uguualmente, è priva di apprezzamento la tesi, peraltro non provata dal Comune, che la reclamante avesse già reso noti alla stampa i propri dati personali contenuti nella determinazione, così come la tesi che la sentenza di condanna in sede penale, da cui era scaturito il procedimento disciplinare nei confronti della reclamante, "era già stata tolta dalla sfera della riservatezza ab origine dal giudice comminando la pena accessoria della pubblicazione" del dispositivo della sentenza su due quotidiani. I soggetti pubblici possono, infatti, diffondere dati personali solo nei casi previsti da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-ter, commi 1 e 3, del Codice), a nulla rilevando che i medesimi dati siano già stati diffusi nell'ambito della pubblicazione di sentenze o provvedimenti a fini di informatica giuridica (cfr. artt. 51 e 52 del Codice) o a titolo di sanzione accessoria, o dallo stesso interessato o da terzi per altre finalità (sul punto, v. provv. n. 35 del 13 febbraio 2020, doc. web n. [9285411](#)).

Pertanto, anche in presenza degli obblighi di pubblicazione ai sensi dell'art. 15 del d.lgs. n. 33/2013, i soggetti chiamati a darvi attuazione non possono comunque "rendere [...] intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione" (art. 7-bis, comma 4, del d.lgs. n. 33/2013). Il Comune avrebbe, pertanto, dovuto pubblicare "gli estremi dell'atto di conferimento dell'incarico" (art. 15, comma 1, lett. a) del d.lgs. n. 33/2013) senza riportare il contenuto integrale dell'atto, né fare alcun riferimento neanche indirettamente all'interessata.

Le medesime considerazioni valgono, altresì, in merito agli obblighi derivanti dall'art. 124 del d.lgs. 267/2000, invocato dal Comune per giustificare la pubblicazione della determinazione nella sezione "Albo pretorio" del proprio sito web istituzionale, atteso che anche alle pubblicazioni nell'albo pretorio online si applicano tutti i limiti previsti sopra menzionati con riguardo al rispetto del principio di minimizzazione dei dati e alle cautele nel caso in cui gli atti da pubblicare contengano dati appartenenti a categorie particolari o giudiziari (cfr. parte II, par. 3(a) delle Linee guida sopra citate). Nella determinazione oggetto di pubblicazione non avrebbero dovuto essere riportati dati identificativi dell'interessata (es. iniziali del nome e del cognome) né altri dati di contesto che avrebbero potuto consentire l'identificazione della stessa, quali, ad esempio, i riferimenti puntuali agli estremi di altri atti e documenti amministrativi. La pubblicazione della determinazione con tali accorgimenti non avrebbe, peraltro, compromesso il principio di adeguata motivazione di cui all'art. 3 della l. 241/1990, poiché la versione integrale della determinazione sarebbe restata, in ogni caso, agli atti del Comune e sarebbe stata accessibile, da parte di soggetti qualificati, nei modi e nei limiti previsti dalla legge.

Peraltro, la circostanza che la determinazione sia stata pubblicata, senza previa anonimizzazione, nella sezione dedicata all'Albo storico, oltre l'arco temporale previsto dalla disciplina di settore (cfr. art. 124, d.lgs. 18 agosto 2000, n. 267 concernente la pubblicità degli atti degli enti locali sull'albo pretorio, nonché art. 32, l. 18 giugno 2009, n. 69), connota ulteriormente di illiceità la diffusione dei dati personali in essa contenuti.

Sanzione: euro 4.000,00

DEBITI FUORI BILANCIO

Provvedimento Garante n. 120 del 02/07/2020
Fattispecie: documento pubblicato sul sito web istituzionale contenente dati personali dei segnalanti (nominativo e residenza), relativi a un debito maturato dalla Regione nei loro confronti in esecuzione di una sentenza esecutiva con specificazione dell'ammontare.
Violazioni: <u>violazione del principio di minimizzazione dei dati e assenza di idonei presupposti normativi, in violazione dei principi di base del trattamento</u> contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD, nonché dell'art. 19 comma 3 del Codice (vigente all'epoca dei fatti e il cui contenuto è ora riprodotto nei medesimi termini nel nuovo art. 2-ter, commi 1 e 3, del Codice).
Sanzione: euro 4.000,00

DEFUNTI

Parere Garante n. 2 del 10/01/2019
Fattispecie: Il RPT di una ASL ha richiesto al Garante nell'ambito del procedimento relativo a una richiesta di riesame di un provvedimento di diniego di un accesso civico in merito a un'istanza di accesso ai sensi del d. lgs. n. 33/2013 « <u>agli atti di audit clinico e successiva elaborazione del percorso clinico da parte del risk manager, inerente il caso segnalato [dal soggetto istante all'Azienda], riguardante la discrepanza tra rilievo autoptico e diagnosi clinica</u> » effettuata su un paziente. <u>L'amministrazione ha negato l'accesso</u> , rappresentando che «la documentazione contiene dati sensibili personali e quindi non accessibili sulla base della normativa [sopra] richiamata». <u>La documentazione oggetto dell'accesso civico contiene dati e informazioni personali, inerenti il quadro clinico di un paziente deceduto, con specifici e accurati dettagli su ricovero, degenza, sintomi, anamnesi, diagnosi, esami effettuati (di cui alcuni particolarmente invasivi) con relativi risultati, terapia, farmaci somministrati, consulenze mediche effettuate, nonché informazioni sul credo religioso professato.</u> I documenti oggetto dell'accesso civico contengono indubbiamente "dati relativi alla salute" di un paziente, anche se poi deceduto.
Contenuto parere: In relazione ai «dati personali delle persone decedute», la normativa europea in materia di protezione dei dati personali, pur prevedendo che il Regolamento non trovi a essi applicazione, stabilisce – con una "clausola di salvaguardia" – che « <u>Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute</u> » (considerando n. 27). Al fine di dare applicazione alla descritta facoltà prevista dal Regolamento europeo, il legislatore italiano ha sancito che « <u>I diritti di cui agli articoli da 15 a 22 del Regolamento</u> », laddove « <u>riferiti ai dati personali concernenti persone decedute</u> », « <u>possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione</u> » (art. 2-terdecies, comma 1, del Codice, introdotto dall'art. 2, comma 1, lett. f, del d. lgs. n. 101 del 10/8/2018). Ne consegue che <u>ai dati personali concernenti le persone decedute continuano ad applicarsi le tutele previste dalla disciplina in materia di protezione dei dati personali di cui al RGPD e al Codice della Privacy.</u> In tale contesto, si osserva che il Codice, a tutela dei singoli e nel «rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona» (art. 1, comma 1), prevede un <u>espresso "divieto di diffusione", ossia della possibilità di dare «conoscenza [...] a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione» di "dati relativi alla salute"</u> (art. 2-septies, comma 8; art. 2-ter, comma 4, lett. b), all'interno dei quali nella fattispecie sottoposta all'attenzione del Garante – per i motivi sopra riportati – rientrano anche quelli riferiti al <u>paziente deceduto</u> , contenuti nella documentazione oggetto dell'accesso civico. Per tutto quanto evidenziato, si rileva quindi che <u>un eventuale accoglimento dell'istanza di accesso civico alla documentazione richiesta comporterebbe la conoscenza di "dati relativi alla salute", per i quali come detto è invece previsto un espresso divieto di diffusione</u> (art. 2-septies, comma 8, del Codice. Cfr. anche art. 7-bis, comma 6, del d. lgs. n. 33/2013, che al riguardo prevede, analogamente, come «Restano fermi i limiti [...] alla diffusione dei dati idonei a rivelare lo stato di salute [...]»)). La vicenda esaminata rientra, dunque, in una delle ipotesi di "esclusione dell'accesso civico" previste dalla normativa statale in materia di trasparenza, che prevede espressamente come l'accesso civico deve essere escluso nei «casi di divieti di accesso o divulgazione previsti dalla legge» (art. 5-bis, comma 3, del d. lgs. n. 33/2013). Quanto riportato è confermato anche dalle Linee guida dell'Anac in materia di accesso civico con riferimento alle « <u>Eccezioni assolute</u> » all'accesso civico, laddove è indicato che «Nella valutazione dell'istanza di accesso,

l'amministrazione deve [...] verificare che la richiesta non riguardi atti, documenti o informazioni sottratte alla possibilità di ostensione o ad accesso "condizionato" in quanto ricadenti in una delle fattispecie indicate nell'art. 5-bis co. 3» (par. 6). Nello specifico, nel par. 6.2., intitolato «Altri casi di segreto o di divieto di divulgazione», è altresì precisato che «[...] alcuni divieti di divulgazione sono previsti dalla normativa vigente in materia di tutela della riservatezza con riferimento a: dati idonei a rivelare lo stato di salute, ossia a qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici (art. 22, comma 8, del Codice [oggi art. 2-septies, comma 8]; art. 7-bis, comma 6, d. lgs. n. 33/2013)».

si ritiene che – conformemente ai precedenti orientamenti del Garante (cfr. i pareri resi nei provvedimenti n. 188 del 10/4/2017, in www.gpdp.it, doc. web n. [6383249](#); n. 206 del 27/4/2017, ivi, doc. web n. [6388689](#); n. 98 del 22/2/2018, ivi, doc. web n. [8165944](#); n. 226 del 16/4/2018, ivi, doc. web n. [8983848](#)) – l'Azienda sanitaria, anche se con una sintetica motivazione, ha correttamente respinto l'istanza di accesso civico, in conformità alla disciplina in materia di protezione dei dati personali

DELIBERAZIONI

Provvedimento Garante: n. 73 del 25/02/2021

Fattispecie: documenti riguardanti le domande poste all'amministrazione nel question time presentato dal reclamante e le risposte fornite dall'amministrazione. Tali documenti contenevano dati e informazioni personali del reclamante, fra cui, oltre nome e cognome, anche data e luogo di nascita, residenza, p.e.c., numero di telefono cellulare, firma autografa.

L'ANAC rappresenta, in via preliminare, riserve in ordine alla possibilità che l'art 45-bis del Regolamento del Consiglio Comunale, prima richiamato, possa costituire un'ideale base normativa per la diffusione dei dati personali ai sensi dell'art. 2-ter, commi 1 e 3, del Codice, soprattutto nel caso in cui le domande poste non siano poi ammesse e discusse nel corso del Consiglio comunale.

Violazioni: diffusione illecita in quanto i dati personali non «limitati a quanto necessario rispetto alle finalità per le quali sono trattati», in violazione dell'art. 5, par. 1, lett. c), del RGPD e del principio di «minimizzazione dei dati».

Sanzione: euro 2.000

DIRITTI DELL'INTERESSATO

Provvedimento Garante n. 183 del 15/10/2020

Fattispecie: istanza per l'esercizio di accesso ai propri dati personali a seguito di un verbale di accertamento di violazione al codice della strada rilevata con sistema di videosorveglianza.

Violazioni: ritardato (dopo quasi un anno) riscontro all'istanza di accesso violando il termine di 30 giorni previsto dall'art. 12 del RGPD, senza, peraltro, aver informato il reclamante dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale entro il medesimo termine.

Sanzione: euro 2.000

Provvedimento Garante n. 139 del 15/04/2021

Fattispecie: mancato riscontro a istanza diretta all'esercizio del diritto di accesso.

Violazioni: mancato riscontro in violazione gli artt. 5, par. 1, lett. a), 12 e 15 del Regolamento per non aver fornito nei termini di legge il dovuto riscontro all'interessato, con riferimento all'esercizio del diritto di accesso.

Sanzione: euro 12.000,00

Provvedimento Garante n. 141 del 15/04/2021

Fattispecie: reclamo interessato per mancato riscontro alla sua istanza diretta all'esercizio del diritto di accesso.

Violazioni: il titolare del trattamento ha dato riscontro alla richiesta di esercizio del diritto di accesso ai dati personali, ben oltre il termine di un mese previsto dall'art. 12 del Regolamento, senza, peraltro, aver informato il reclamante dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale entro il medesimo termine.

Sanzione: euro 2.000,00

Provvedimento Garante n. 157 del 12/03/2015
Fattispecie: richiesta di ottenere la conferma dell'esistenza dei dati personali che lo riguardano relativi agli ultimi dieci anni , nonché la comunicazione degli stessi in forma intellegibile con trasposizione su supporto cartaceo;
Violazioni: <u>la facoltà del titolare del trattamento di fornire riscontro all'interessato attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti ai sensi dell'art. 10, comma 4, del Codice, non trasforma l'istanza di accesso ai dati personali in un'istanza di accesso ai documenti</u> , in quanto è semplicemente diretta ad agevolare il riscontro da parte del titolare medesimo. <i>(Nel caso di specie il titolare del trattamento era un Comune contro cui l'interessato aveva proposto ricorso finalizzato ad ottenere la comunicazione dei dati personali in forma intellegibile con trasposizione su supporto cartaceo).</i>
Sanzione: condanna alle spese per euro 500,00

ELETTORALE

Provvedimento Garante: n. 96 DEL 18/04/2019
Fattispecie: Con questo provvedimento il Garante richiama l'attenzione sui principali casi nei quali partiti, organismi politici, comitati di promotori e sostenitori nonché singoli candidati, possono utilizzare i dati personali degli interessati per iniziative di propaganda nel rispetto dei diritti e delle libertà fondamentali degli interessati (art. 1, par. 2, Regolamento). Di seguito sono evidenziati, distintamente ai paragrafi 2 e 3, i presupposti di liceità del trattamento dei dati nell'ambito dell'attività elettorale (consenso, legittimo interesse e altri presupposti) per iniziative di propaganda elettorale e connessa comunicazione politica.

INCARICO LEGALE

Provvedimento Garante n. 1 del 02/07/2020
Fattispecie: determinazione , pubblicata all'Albo pretorio online e nell'archivio storico dell'Albo, di affidamento incarico ad un legale per resistere ad un ricorso al TAR proposto da una dipendente per essere stata esclusa da <u>procedura di mobilità</u> per avere omesso nell'autodichiarazione di avere riportato una condanna penale
Violazioni: <u>assenza di idonei presupposti normativi</u> , in violazione degli artt. 6, paragrafo 1, lett. c) ed e), 2 e 3, lett. b), e 2-ter, commi 1 e 3, del Codice, <u>nonché dei principi di base del trattamento</u> contenuti nell'art. 5, par. 1, lett. a) e c) del RGDP; poiché <u>nella determinazione erano presenti anche dati relativi a reati (con contestuale richiamo a un atto amministrativo contenente dati relativi a condanne penali e reati)</u> , la pubblicazione è avvenuta anche in violazione dell'art. 10 del RGDP, nonché dell'art. 2-octies del Codice.
Sanzione: euro 4.000,00

INFORMATIVA

Provvedimento Garante n. 132 del 05/03/2015
Fattispecie: avviso sui giornali con invito a presentare curriculum per assunzioni
Violazioni: mancata informativa
Sanzione: euro 18.000,00

NOTIFICAZIONE ATTI

Provvedimento Garante n. 39 del 27/01/2021
Fattispecie: pubblicazione nell'Albo pretorio di un atto che riporta i dati del debitore che non ha versato il corrispettivo per la mensa di un minore di anni 9 e della madre , in quanto essendo senza fissa dimora il Comune ha concesso il domicilio all'indirizzo anagrafico convenzionale in conformità ad una delibera della Giunta che in materia di notificazione non può derogare alle norme primarie del codice civile (art. 140) che non consente la pubblicazione <u>integrale dell'atto</u> .
La pubblicazione sull'albo pretorio è avvenuta in quanto la signora destinataria dell'XX era soggetto "senza fissa

dimora”, ed è stato quindi applicato il punto 6 della Deliberazione di Giunta n. 31 del 3 marzo 2017 «Sistema di iscrizione anagrafica delle persone senza dimora presenti abitualmente sul territorio di », nella parte in cui è previsto che le notifiche nei confronti dei residenti senza fissa dimora è «sostituita dalla pubblicazione presso l’Albo pretorio di dell’atto o della comunicazione indirizzati al destinatario» ed è «eseguita trascorso il trentesimo giorno di pubblicazione».

Il Garante ritiene che la predetta delibera di Giunta non ha natura regolamentare e, inoltre, non può derogare alla normativa di rango primario dettata dal legislatore in materia di notificazione degli atti giudiziari», con la conseguenza che rimangono applicabili anche per i soggetti «senza fissa dimora» le disposizioni contenute negli artt. 140 ss. del c.p.c. (per la notifica degli atti giudiziari) e dell’art. 60 del d.P.R. n. 600 del 19/9/1973 (per la notifica degli atti tributari).

Violazioni: La diffusione integrale del documento contenente i dati personali del minore e della madre è avvenuto:

- in maniera non conforme al rispetto dei principi di “liceità” e “minimizzazione” del trattamento, in violazione dell’art. 5, par. 1, lett. a) e c), del RGPD;
- in assenza di un idoneo presupposto normativo, in violazione dell’art. 2-ter, commi 1 e 3, del Codice e dell’art. 6, par. 1, lett. c) ed e); par. 2 e par. 3, lett. b), del RGPD.

Sanzione: euro 10.000,00

ORDINANZE SINDACALI

Provvedimento Garante n. 21 dell’11/03/2021

Fattispecie: **ordinanza sindacale di sgombero immobili comunali**, pubblicata all’Albo pretorio online

Violazioni:

- diffusione di dati (nominativo, data e luogo di nascita, codice fiscale, residenza) “non limitati alla finalità del trattamento” in violazione del principio di “minimizzazione” dei dati ex art. 5, prf. 1, lett. c) RGDP
- assenza di presupposto normativo per la pubblicazione eccedente i 15 giorni prescritti dall’art. 124, c.1, d.lgs. 267/2000
- violazione dei principi base del trattamento ex artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD

Sanzione: euro 3.000,00

PERSONALE

Provvedimento Garante n. 256 del 24/06/2021

Fattispecie: delibera GM per avvio **procedimento disciplinare nei confronti di dipendente**, pubblicata all’Albo pretorio e nella sezione Amministrazione Trasparente

Violazioni: assenza di idoneo presupposto normativo per la pubblicazione eccedente i 15 giorni ex art. 124, c.1, d.lgs. 267/2000;

illecita pubblicazione di dati, informazioni e documenti non avendo il Comune l’obbligo di pubblicare ai sensi del d.lgs. n. 33/2013 ed essendo una pubblicazione facoltativa avrebbe dovuto anonimizzare tutti i dati personali presenti, violando così l’art. 7-bis, c. 3, d.lgs. 33/2013.

Sanzione: euro 1.000,00

Provvedimento Garante n. 69 del 25/02/2021

Fattispecie: determina afferente al **rapporto di lavoro e alla vita privata di una dipendente**, pubblicata nell’Albo pretorio online

Violazioni:

- assenza di idoneo presupposto normativo per la pubblicazione eccedente i 15 giorni prescritti dall’art. 124, c.1, d.lgs. 267/2000
- illecita diffusione di dati personali relativi a vicende connesse al rapporto di lavoro e alla vita privata della dipendente in essa contenuti. (cfr. Cass. civ., sez. II, ord. n. 18292 del 3 settembre 2020) in violazione del principio di minimizzazione dei dati ex art. 5, prf. 1, lett. c) RGDP

Sanzione: euro 2.000,00

Provvedimento Garante n. 108 del 25/03/2021
Fattispecie: Delibere e determine relative all' organizzazione della Polizia Locale , pubblicate nella sezione "Archivio Albo pretorio" dell'Unione di Comuni , <u>contenenti dati e informazioni personali dei reclamanti, agenti di polizia municipale, quali nome e cognome, grado, indicazione della sede di lavoro e tipodi mansioni/competenze svolte.</u>
Violazioni: ➤ <u>illecita diffusione</u> di dati e informazioni personali degli agenti di polizia municipale (quali nome e cognome, grado, sede di lavoro e tipo di mansioni/competenze) <u>in assenza di idonei presupposti normativi, per il periodo eccedente i 15 giorni</u> previsti dall'art. 124, comma 1, del d. lgs. n. 267/2000, in violazione dell'art. 2-ter, commi 1 e 3 del Codice; il Garante non ritiene giustificata la pubblicazione, come sostenuto dall'Unione, ai sensi dell'art. 13 del d.lgs. 33/2013 che fa riferimento in generale all'«organizzazione delle pubbliche amministrazioni» e non alla pubblicazione dei dati personali del personale dipendente o degli agenti di polizia municipale; né nell'art. 8, comma 3, del medesimo decreto che si riferisce ai soli atti e documenti pubblicati ai sensi della normativa in materia di trasparenza nella sezione Amministrazione trasparente; e ritiene rilevante quanto sostenuto dai vigili urbani reclamanti: «non vi è alcun interesse pubblico a conoscere la precisa identità degli agenti preposti a determinati servizi per la collettività, né cattivo esercizio di potere pubblico nel non comunicarlo. L'unico interesse pubblico riscontrabile è quello di sapere se vi è un determinato servizio, l'ufficio preposto a svolgerlo, la sua ubicazione e l'esistenza e il numero di addetti in tale posizione e quanto l'ente investe su tali servizi. Così come, un adeguato esercizio del pubblico potere di cui è investito il titolare del trattamento può essere ben realizzato con il fornire tali informazioni, senza indicare l'identità degli agenti di Polizia Locale». ➤ <u>violazione del principio di minimizzazione</u> dei dati ex art. 5, par. 1, lett. c), del RGPD; ➤ <u>violazione dei principi base del trattamento</u> ex artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD.
Sanzione: euro 13.000,00

Provvedimento Garante n. 42 del 26/02/2020
Fattispecie: provvedimenti del direttore generale inerenti l' assenza ingiustificata a visita di controllo e a riconoscimento invalidità pubblicati sul sito web istituzionale
Violazioni: <u>illecita diffusione di dati sensibili</u> (informazioni e dettagli sulle visite fiscali effettuate nel caso di assenza dal lavoro per motivi di salute e indicazione delle relative date, sulle visite ambulatoriali, sulla patologia sofferta), <u>in violazione degli obblighi e dei principi di base del trattamento</u> contenuti negli artt. 5, par. 1, lett. a) e c); 9, parr. 2 e 4, del RGPD, nonché dell'art. 2-septies, c. 8, del Codice.
Sanzione: euro 6.000,00

Provvedimento Garante n. 35 del 13/02/2020
Fattispecie: atti e documenti pubblicati sul sito web istituzionale contenenti dati personali anche relativi alla salute di una dipendente.
Violazioni: <u>violazione dei principi di "liceità, correttezza e trasparenza"</u> nonché di "minimizzazione" del trattamento, in violazione dell'art. 5, par. 1, lett. a) e c), del Regolamento; <u>assenza di presupposto normativo</u> , in violazione dell'art. 2-ter, commi 1 e 3, del Codice e dell'art. 6, par. 1, lett. c), e), par. 2 e par. 3, lett. b), del Regolamento; <u>violazione del divieto di diffusione dei dati sulla salute</u> di cui all'art. 2-septies, comma 8, del Codice.
Sanzione: euro 4.000,00

POLIZIA LOCALE

Provvedimento Garante: n. 137 del 09/07/2020
Fattispecie: il reclamante ha lamentato che : - gli scatti fotografici siano stati effettuati durante una manifestazione in area pubblica e ritraggono una persona in divisa che riveste un ruolo pubblico; - la loro diffusione su Facebook ha avuto una finalità denigratoria, finalizzata a strumentalizzazione politica; - la loro pubblicazione, che ha suscitato commenti ironici e allusivi, è avvenuta senza alcuna autorizzazione; e ha chiesto, con riferimento alle foto di cui sopra, di ingiungere al titolare o al responsabile del trattamento di soddisfare le richieste di cui all'art. 17 del Regolamento;
Elementi delle foto pubblicate: sulla pagina Facebook dell'Associazione XXX sono state diffuse due fotografie che

ritraggono il reclamante, comandante della polizia locale di, durante l'evento ".....";
l'autore della diffusione su Facebook ha dichiarato che le foto pubblicate nel post si inseriscono nell'ambito di una serie di critiche rivolte all'amministrazione comunale di e alla sua gestione della polizia locale, ritraendo il comandante della polizia locale di mentre prestava servizio in divisa durante un evento ludico di portata provinciale ".....", svoltosi la sera del, a, vicino alla sua abitazione, ma al di fuori del territorio di sua competenza, sottolineando come invece a, la mattina successiva, a un evento di portata regionale, ".....", non vi fosse alcun agente di polizia locale in servizio;

Contenuto del parere:

- l'art. 5, par. 1, lett. a), del Regolamento, che enuncia il principio generale di liceità e correttezza del trattamento dei dati;

- l'art. 137, comma 3, del Codice, in base al quale:

• il giornalista – al pari di questi chiunque proceda alla pubblicazione o diffusione anche occasionale di articoli, saggi e altre manifestazioni del pensiero – può diffondere dati personali, anche senza il consenso dell'interessato, purché ciò avvenga nei limiti posti al diritto di cronaca e, in particolare, nel rispetto del requisito «dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico»;

• «possono essere trattati i dati personali relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico»;

- l'art. 6, comma 2 delle Regole deontologiche, ai sensi del quale “la sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica”;

l'art. 97 della legge 22 aprile 1941, n. 633 (legge sulla protezione del diritto d'autore) prevede che non occorra il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico;

- nel caso in esame risulta sussistente l'interesse pubblico, in quanto nelle foto si al fine di comprovare una critica nei confronti dell'amministrazione comunale in merito alla gestione della polizia locale;

- le foto non risultano lesive della dignità o della riservatezza persona, limitandosi a ritrarre il reclamante, in divisa e a fianco di un collega, in orari diversi, mentre cammina nel corso della manifestazione;

Parere Garante n. 180 del 15/10/2020

Fattispecie: il Responsabile della prevenzione della corruzione e della trasparenza (RPCT) del Comune di ha chiesto al Garante il parere previsto dall'art. 5, comma 7, del d. lgs. n. 33/2013, nell'ambito del procedimento relativo a una richiesta di riesame di un cittadino su un provvedimento di accoglimento parziale a una propria istanza di accesso civico presentata al Comune di

Dall'istruttoria risulta che è stata presentata una richiesta di accesso civico – ai sensi dell'art. 5 comma 2, del d. lgs. n. 33/2013 – avente a oggetto il **rilascio di copia dei seguenti documenti afferenti il personale dell'Ufficio ricorsi all'Autorità Giudiziaria” della Polizia Locale:**

«a) Ordini di servizio definitivi (ovvero quelli in base ai quali vengono calcolati gli emolumenti stipendiali), previo oscuramento dei nomi dei dipendenti, per il periodo intercorrente dal al

b) Registro delle variazioni agli ordini di servizio (altrimenti denominato “brogliaccio”), previo oscuramento dei nomi dei dipendenti per il periodo intercorrente dal al

c) Tutte le disposizioni formali scritte rivolte specificamente al personale relativa all'anno 2019, previo oscuramento di eventuali nomi dei dipendenti».

L'amministrazione ha accordato un accesso civico parziale ai soli documenti di cui alla lettera c) fornendo le «disposizioni formali scritte, rivolte nel 2019 al personale, in forza all'ufficio della Polizia Locale del Comune di», rifiutando invece le altre richieste per motivi inerenti alla protezione dei dati personali e all'impossibilità di anonimizzare la documentazione richiesta.

Contenuto del parere : la relativa ostensione, anche considerando il particolare regime di pubblicità dei dati e informazioni ricevuti tramite l'istituto dell'accesso civico (cfr. art. 3, comma 1, d. lgs. n. 33/2013), potrebbe determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà del personale appartenente alla Polizia locale, in violazione del principio di minimizzazione dei dati (art. 5, par. 1, lett. b e c, del RGPD), arrecando proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Al riguardo, si deve infatti tenere conto della tipologia e della natura dei dati e delle informazioni personali, anche di dettaglio, contenuti negli ordini di servizio – di tipo preventivo e consuntivo – richiesti, quali per ogni singolo lavoratore, come descritto dal RPCT: turno di servizio previsto, lavoro svolto, attività da svolgere nel giorno seguente, prestazioni effettive, alla luce delle eventuali variazioni intervenute, dati su eventuali assenze programmate o su

assenze dal servizio comunicate a seguito di malattie o infortuni, posizione lavorativa del dipendente, turno di riposo, prestazione svolta in regime di straordinario, permessi fruiti anche ai sensi della legge n. 104/92, etc.

La generale conoscenza, derivante da un eventuale accoglimento della richiesta di accesso civico ai predetti dati e informazioni, inerenti aspetti molto particolareggiati dell'attività lavorativa svolta, può essere fonte di rischi specifici per i soggetti interessati, anche considerando la possibile ricostruzione della vita e delle abitudini dei soggetti appartenenti al personale appartenente alla Polizia locale del Comune di Milano addetto all'Ufficio Ricorsi all'Autorità Giudiziaria (che peraltro non risulta essere stato coinvolto nel procedimento relativo all'accesso civico come controinteressato), determinando possibili ripercussioni negative sul piano personale, professionale, sociale e relazionale, sia all'interno che all'esterno dell'ambiente lavorativo. Bisogna, inoltre, tener conto delle ragionevoli aspettative di confidenzialità dei controinteressati in relazione al trattamento dei propri dati personali al momento in cui questi sono stati raccolti dal Comune, nonché della non prevedibilità, al momento della raccolta dei dati, delle conseguenze derivanti, al personale appartenente alla Polizia locale, dall'eventuale conoscibilità, da parte di chiunque, dei dati richiesti tramite l'accesso civico (cfr. par. 8.1 delle Linee guida dell'ANAC in materia di accesso civico, cit.).

Al riguardo, non è possibile accordare – come invece domandato dal soggetto istante nella richiesta di riesame – neanche un accesso civico parziale, oscurando i nominati dei soggetti interessati. Ciò in quanto tale accorgimento non elimina del tutto la possibilità – come evidenziato anche dal RPCT – che questi ultimi possano essere re-identificati, anche all'interno dello stesso luogo di lavoro, tramite gli ulteriori dati di dettaglio e di contesto contenuti nella documentazione richiesta o mediante altre informazioni in possesso di terzi.

Provvedimento Garante: n. 107 del 24/03/2022

Fattispecie: la piattaforma utilizzata dal corpo di Polizia locale del Comune di per la gestione delle contravvenzioni al Codice della Strada, le cui licenze sono state acquistate dalla Società XXX, contenente i dati personali dei cittadini destinatari di contravvenzioni, è stata oggetto di un accesso abusivo, da parte di soggetti non autorizzati, cagionato "dall'incauto comportamento di alcuni agenti, che violando le disposizioni di servizio, non avrebbero modificato la password di primo accesso e divulgato l'URL di accesso".

Violazioni: La società, proprio in ragione della sua esperienza nel settore, era tenuta a verificare costantemente l'efficacia delle misure poste a presidio della piattaforma fornita alla Polizia Locale e avrebbe comunque dovuto adottare misure tecniche e organizzative volte ad assicurare che le password dei soggetti autorizzati rispettassero criteri di qualità e fossero obbligatoriamente modificate al primo utilizzo.

Il servizio in questione era disponibile anche su protocollo http, ossia tramite un protocollo di rete che non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato;

risulta accertata la mancata adozione, da parte della società, di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, in violazione degli artt. 5 par. 1 lett. f), e 32 del Regolamento.

Sanzione: euro 10.000,00 comminata alla ditta fornitrice del software di gestione delle contravvenzioni

PLURINDIRIZZI

Provvedimento Garante n. 1 del 09/01/2020

Fattispecie: una e-mail contenente una comunicazione mediante un unico messaggio di posta elettronica indirizzato a un numero plurimo di destinatari (16), i cui indirizzi sono stati inseriti nel campo copia conoscenza (c/c), **ha, di fatto, senza giustificato motivo e in assenza di qualsivoglia presupposto normativo, rivelato reciprocamente, alle famiglie coinvolte, lo stato di inadempimento dei minori rispetto agli obblighi vaccinali**; tale comunicazione di dati sulla salute si sarebbe potuta evitare inserendo gli indirizzi dei destinatari nel campo denominato "copia conoscenza nascosta" (ccn);

Violazioni: s (v. anche art. 2-sexies del Codice) e in s (artt. 5 e 9 del Regolamento);

Sanzione: soltanto un ammonimento a conformare il trattamento al Regolamento UE

PROCEDIMENTO DISCIPLINARE

Provvedimento Garante n. 256 del 24/06/2021

Fattispecie: pubblicazione, anche oltre il termine dei 15 giorni prescritto dall'art. 124 del TUEL, nella sezione storica dell'Albo pretorio che non aveva l'obbligo di pubblicare, ai sensi del d.lgs. n. 33/2013, di una delibera contenente dati personali e valutazioni sull'operato di un dipendente del Comune. In particolare nella **delibera il Comune invitava "il responsabile dei procedimenti disciplinari ad attivare un procedimento disciplinare applicando, se del caso, una sanzione esemplare"**.

Il Comune, se avesse voluto pubblicarla ai sensi del d.lgs. n. 33/2013 avrebbe dovuto anonimizzare tutti i dati che potevano rendere identificabile il dipendente.

Il Comune non ha comprovato l'esistenza di una specifica norma di legge che stabilisca la pubblicazione della determina della Giunta comunale, contenente informazioni riguardanti l'intenzione di avviare un procedimento disciplinare nei confronti di un dipendente. Peraltro, anche in presenza di una norma di legge che preveda la pubblicazione di atti e documenti della pubblica amministrazione (cfr. art. 124 del d.lgs. 18 agosto 2000, n. 267) – che in ogni caso deve essere attuata anche con riguardo all'arco temporale di pubblicazione da questa stabilito – devono essere, comunque, rispettati i principi di protezione dei dati, tra i quali il principio di "minimizzazione dei dati" (art. 5, par. 1, lett. c), del Regolamento.

Violazioni: diffusione dei dati personali relativi al reclamante, contenuti nella deliberazione della giunta comunale in assenza di idonei presupposti normativi, in violazione dell' art. 6 del Regolamento e 2-ter, commi 1 e 3, del Codice, nonché dei principi di base del trattamento contenuti nell'art. 5, par. 1, lett. a) e c) del Regolamento.

Sanzione: euro 1.000,00

PROGRAMMI DI ACCESSO A SERVIZI

Provvedimento Garante n. 48 dell'11/02/2021

Fattispecie: i permessi per l'accesso e la sosta nelle zone a traffico limitato ("Z.T.L."), da esporre sui veicoli, riportano sul frontespizio un c.d. QR code, che consente a chiunque, mediante l'utilizzo di una generica applicazione per dispositivi mobili (mobile app) in grado di decodificarne il contenuto, di accedere a dati personali relativi al titolare del permesso Z.T.L. o al suo utilizzatore; e, addirittura, anche ad altri titolari di permesso Z.T.L.;

le informazioni riportate "in chiaro" (non codificate nel QR code) sul contrassegno riguardano: la tipologia di autorizzazione (es. accesso, sosta, scarico merci, etc.), la targa del veicolo, il numero del permesso e la validità temporale; nel QR code sono invece riportate: la categoria del richiedente (es. domiciliato, distributore di merci, proprietario di posto auto, etc.), la ragione o denominazione sociale o istituzionale (in caso di veicolo appartenente a persona giuridica) o il nome e cognome (in caso di persona fisica) del titolare del permesso, nonché il nome e cognome dell'utilizzatore dello stesso;

Violazioni: illecito trattamento di dati personali effettuato, in quanto esso è avvenuto in maniera non conforme ai principi generali del trattamento, in assenza di un'idonea base giuridica, nonché in assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, in violazione dell'art. 32 del RGDP.

Sanzione: euro 60.000,00

Provvedimento Garante n. 140 del 15/04/2021

Fattispecie: piattaforma informatica denominata utilizzata per gestire le offerte alimentari a favore delle famiglie bisognose, accessibile dal sito del Comune.

Il Comune si è avvalso del supporto di soggetti esterni (Enti del Terzo Settore, Sindacati e Parrocchie) dislocati strategicamente a coprire l'intero territorio cittadino al fine di garantire "assistenza agli utenti nella compilazione della richiesta per l'erogazione dei buoni spesa per l'emergenza epidemiologica da Covid-19", in ausilio alla Centrale della Protezione Civile Comunale".

Ogni OpT è stato designato Responsabile del trattamento.

A seguito della creazione della scheda individuale e della compilazione dell'autocertificazione, da parte del richiedente direttamente sull'apposita piattaforma messa a disposizione dal Comune, "La routine a disposizione dei punti di raccolta (OpT) abilita i responsabili ivi incaricati ad interrogare il database tramite l'inserimento del codice fiscale dell'utente per accedere alla scheda individuale e, verificata la corrispondenza tra il numero di pratica assegnato dalla piattaforma all'autodichiarazione con quello riportato sulla copia cartacea sottoscritta, nonché la presenza di un valido documento di identità, effettuavano la conferma di ricezione della pratica. La routine permette

anche la ricerca non massiva con almeno i primi 3 caratteri del codice fiscale per favorire l'individuazione delle schede individuali dei cittadini che non portavano con sé il numero di codice fiscale. L'interrogazione delle schede visualizza anche i passaggi salienti dello stato di avanzamento della pratica, senza fornire dettagli sugli eventuali step non superati".

A ciascuna OpT era stata attribuita dal Comune per l'accesso alla piattaforma uniche credenziali, non modificabili, che non consentivano l'attribuzione univoca delle operazioni di trattamento svolte dai diversi operatori turnanti presso l'OpT a una persona fisica responsabile delle medesime.

Violazioni: non sono state adottate le misure tecniche e organizzative adeguate per la protezione dei dati personali, in quanto era possibile, per un operatore autorizzato di qualsiasi OpT, consultare tutte le pratiche inserite nella citata piattaforma, visualizzare i dati anagrafici e la fascia economica ISEE dei richiedenti il buono alimentare e apprendere, di conseguenza, la condizione e situazione di fragilità economica in capo ai richiedenti medesimi.

Si sarebbe dovuto attribuire una credenziale di accesso diversa per ogni operatore di ciascuna OpT in modo da consentire al programma di registrare le operazioni effettuate da ciascun operatore.

Violazione per misure non previste e non attuate:

- violazione del principio di "integrità e riservatezza", di cui all'art. 5, par. 1, lett. f), del Regolamento, in quanto non è stata assicurata un'adeguata sicurezza dei dati personali, avendo consentito accessi non autorizzati;
- violazione dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, di cui all'art. 25 del RGDP;
- assenza di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, in violazione dell'art. 32 del RGDP, in quanto non si è tenuto in adeguato conto dei rischi di accessi non autorizzati;

Sanzione: euro 40.000,00

Provvedimento Garante n. 49 dell'11/02/2021

Fattispecie: il Comune svolge attraverso una propria società la **gestione dei permessi per l'accesso e la sosta nelle zone a traffico limitato ("Z.T.L.")**;

i permessi riportano sul frontespizio un **c.d. QR code**, che consente a chiunque, mediante l'utilizzo di una generica applicazione per dispositivi mobili (mobile app) in grado di decodificarne il contenuto, di accedere a dati personali relativi al titolare del permesso Z.T.L. o al suo utilizzatore, tra cui: la denominazione sociale o istituzionale (es. Questura, scuola elementare) oppure il nome e il cognome (nel caso di persona fisica) del titolare del permesso, il nome e il cognome dell'utilizzatore del permesso, la categoria del richiedente (es. artigiano, lavoratore orari notturni), nonché la targa del veicolo autorizzato.

Ciò accadeva in quanto il servizio online di verifica dei permessi Z.T.L. risultava liberamente accessibile, non essendo protetto da alcuna procedura di autenticazione.

Inoltre, il Comune ha affidato alla propria società il servizio di hosting e di manutenzione di data base e connettività, la quale società ha trattato "dati personali" (art. 4, par. 1, n. 1), del Regolamento), effettuandone la registrazione e la conservazione.

Violazioni:

la diffusione dei predetti dati personali, a partire dal 1° dicembre 2016 (data a decorrere dalla quale è operativo, per i permessi Z.T.L, il formato cartaceo riportante un QR code e il relativo servizio online di verifica), è avvenuta in maniera non conforme ai principi di base di protezione dei dati, nonché in assenza di un idoneo presupposto normativo, in violazione degli artt. 5 e 6 del Regolamento e dell'art. 2-ter del Codice.

Sulla base degli elementi sopra riportati, deve quindi ritenersi che le operazioni sopra descritte diano luogo a un trattamento di dati personali da parte di ZZZ (cfr. "Guidelines 7/2020 on the concepts of controller and processor in the GDPR", adottate dal Comitato europeo per la protezione dei dati il 2 settembre 2020, nella versione sottoposta a consultazione pubblica, in particolare, par. 2.1.4, punto 38, nella parte in cui è riportato l'esempio relativo agli "hosting services"), e che, pertanto, il ricorso da parte del Comune di ai servizi offerti da ZZZ – in assenza di un contratto o altro atto giuridico che disciplinasse il trattamento di dati personali da parte di ZZZ, quale responsabile del trattamento – sia avvenuto in violazione dell'art. 28 del Regolamento.

Sanzione: euro 350.000,00

PROTOCOLLO

Provvedimento Garante n. 418 del 11/07/2018
Fattispecie: <u>tutti i dipendenti del Comune avevano accesso al sistema di protocollazione, potendo così visionare documenti contenenti dati personali anche di natura sensibile e giudiziaria, riferiti al reclamante e ad altri dipendenti dell'Ente.</u>
Violazioni: il Comune <u>ha omesso di attribuire ai propri dipendenti, in possesso delle credenziali per l'accesso al sistema medesimo, idonei profili di autorizzazione e abbia, per l'effetto, consentito agli stessi di visionare atti contenenti dati personali anche di natura sensibile e giudiziaria, relativi ad altri dipendenti comunali, violando così le disposizioni ex art. 34, comma 1, lett. c) e d), del Codice – relative, rispettivamente, all'utilizzazione di un sistema di autorizzazione;</u>
Sanzione: euro 10.000,00

PUBBLICAZIONI FACOLTATIVE

Provvedimento Garante n. 292 del 16/05/2018
Fattispecie: pubblicazione da oltre tre anni nell'Albo pretorio online di una determinazione dirigenziale, scaricabile liberamente, nonché nella sezione "Amministrazione trasparente", con cui si stabilisce l'obbligo di un dipendente di astenersi dalla valutazione di una persona - coniuge del dipendente - per conflitto di interessi, in cui sono riportati i dati sia del dipendente che della moglie e la situazione del conflitto di interessi.
Violazioni: <u>mancanza di idoneo presupposto normativo - di legge o di regolamento - per l'avvenuta pubblicazione oltre i 15 giorni prescritti, in quanto la delibera di GC con cui si è deciso di pubblicare tutte le determinazioni all'Albo pretorio online per 15 giorni consecutivi non è un regolamento ma un semplice "atto di indirizzo"; mancata anonimizzazione dei dati personali per il periodo ulteriore ai 15 giorni di pubblicazione;</u>
Sanzione: divieto di protrarre la pubblicazione e per le future pubblicazioni di attenersi alla deliberazione del Garante n. 243/2014.

RAPPORTO DI LAVORO

Provvedimento Garante: n. 129 del 17/03/2016
Fattispecie: rilevazione delle presenze dei dipendenti un sistema biometrico basato sul trattamento di impronte digitali (ricavati, in particolare, da impronte digitali e riconducibili ad interessati individuati o individuabili), <u>senza aver previamente fornito un'adeguata informativa ai dipendenti stessi né aver raccolto il loro consenso.</u> L'utilizzo di tale sistema è stato giustificato dal Comune con la sussistenza di "esigenze di sicurezza" e di certezza nell'attività di verifica della presenza in servizio dei dipendenti. In relazione a ciò è stato fatto riferimento (sebbene non circostanziato) a episodi di abusi – consistenti nello scambio di badge – avvenuti presso Comuni della medesima Regione di appartenenza.
Violazioni: In ordine all'osservanza degli specifici obblighi posti in capo al titolare del trattamento dalla disciplina in materia di protezione dei dati, <u>non risulta essere stata effettuata la notificazione al Garante ai sensi dell'art. 37 del Codice, né è stata presentata la richiesta di verifica preliminare di cui all'art. 17 del Codice (cfr. le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, punto 7.1.).</u> L'istanza di verifica preliminare risulta infatti, nel caso in esame, necessaria in quanto non risultano integrati gli estremi delle fattispecie di esonero previste altresì dal provvedimento generale prescrittivo in tema di biometria n. 513 del 2014, che ha individuato alcune condizioni tassative al ricorrere delle quali può prescindere da tale adempimento.
Sanzione: è stato soltanto vietato l'utilizzo del sistema

Provvedimento Garante n. 146 del 05/06/2019

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 9124510]

Provvedimento Garante n. 35 del 13/02/2020

Fattispecie: sul sito web istituzionale del Comune di era disponibile un documento denominato "XX" (url: http://...). Nella stessa pagina web era altresì reso disponibile, e liberamente scaricabile, il file in formato pdf del **testo integrale della sentenza n. XX (RG n. XX)**.

Violazioni:

Premessa: La disciplina di protezione dei dati personali prevede che i soggetti pubblici, anche qualora operino nello svolgimento dei propri compiti di datori di lavoro, possono trattare i dati personali (art. 4, n. 1, del Regolamento) dei dipendenti, se il trattamento è necessario "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (si pensi a specifici obblighi o compiti previsti dalla legge per finalità di gestione del rapporto di lavoro) 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" (art. 6, par. 1, lett. c) ed e) del Regolamento).

Più specificamente, i datori di lavoro pubblici possono trattare i dati personali dei lavoratori, anche relativi a categorie particolari di dati e relativi alla salute, per adempiere a specifici obblighi o compiti previsti dalla legge per finalità di gestione del rapporto di lavoro (cfr. artt. 9, par. 2, lett. b) e par. 4, e 88 del Regolamento; artt. 2-sexies e 2-septies del Codice) mediante il personale "autorizzato" e debitamente "istruito" in merito all'accesso ai dati personali particolari (artt. 4, par. 10, 29 e 32, par. 4 del Regolamento).

si evidenzia che l'operazione di diffusione di dati personali (come la pubblicazione su Internet), da parte di soggetti pubblici, è ammessa solo quando prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-ter, commi 1 e 3, del Codice) .

Il titolare del trattamento è tenuto, inoltre, a rispettare i principi in materia di protezione dei dati, fra i quali quello di "liceità, correttezza e trasparenza" nonché di "minimizzazione", in base ai quali i dati personali devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" e devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. a) e c), del RGDP).

In particolare, nel rispetto del principio di "minimizzazione dei dati" (art. 5, par. 1, lett. c), del Regolamento), anche in presenza di un obbligo di pubblicazione, i soggetti chiamati a darvi attuazione non possono comunque diffondere i dati personali eccedenti o non pertinenti (cfr., provv. n. 243 del 15 maggio 2014, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, doc. web n. [3134436](#), parte seconda parr. 1 e 3.a.).

In ogni caso, i dati relativi alla salute, ossia quelli "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" (art. 4, par. 1, n. 15), in ragione della particolare delicatezza di tale categoria di dati, "non possono essere diffusi" (art. 2-septies, comma 8 e art. 166, comma 2, del Codice).

Sanzione: euro 4.000,00

RAPPRESENTANTI DI PERSONE GIURIDICHE**Provvedimento Garante n. 107 del 25/03/2021**

Fattispecie: pubblicazione, per oltre tre anni, nell'Albo pretorio online di una determinazione, scaricabile liberamente, con cui si autorizzava lo **svincolo di un bonifico bancario prodotto da una associazione per partecipare ad una gara** per la gestione di uno stadio comunale, da cui era stata esclusa; la determinazione conteneva i nominativi dei soggetti interessati e il codice iban del conto corrente; alla stessa era allegata la nota del presidente dell'associazione contenente i suoi dati identificati e la copia della carta d'identità.

Il Comune non aveva ottemperato alla richiesta di rimuovere almeno la copia della sua carta d'identità.

Violazioni: pur essendo lecita la diffusione dei dati riferiti all'associazione, è stato violato il principio di minimizzazione dei dati, per avere pubblicato i dati personali del presidente; assenza di un fondamento giuridico per la pubblicazione della carta d'identità; nel caso in cui la pubblicazione si protragga oltre i prescritti 15 giorni, tutti i dati personali devono essere anonimizzati;

il Garante evidenzia che le finalità di pubblicazione all'Albo pretorio online e nella sezione "Amministrazione trasparente" sono diverse e quindi le disposizioni del d.lgs. 33/2013 per finalità di trasparenza non attengono alla pubblicità legale propria dell'Albo pretorio online.

Sanzione: euro 4.000,00

REGISTRO ACCESSI CIVICI

Provvedimento Garante : n. 55 dell'11/02/2021
Fattispecie : «sul sito del Comando Generale della Guardia Costiera, [era] possibile visualizzare i dati personali relativi agli accessi civici», in cui «con un visualizzatore PDF embedded ad un browser, ad esempio di Firefox, [era] possibile ottenere una visione momentanea dei campi oscurati con rettangoli bordati di rosso» e «una volta scaricato il file PDF localmente», si poteva «sbloccare i blocchi di sicurezza anche tramite procedure online, ad esempio tramite il sito [identificato in atti]. [Inoltre, il] file ottenuto pot[eva] essere facilmente modificato, rimuovendo le maschere (rettangoli bordati di rosso), con una applicazione [dotata di] funzione di editing dei PDF [...]».
Violazioni : ha effettuato un trattamento di dati personali: - <u>non «limitati a quanto necessario rispetto alle finalità per le quali sono trattati»</u> e non rispettando, quindi, il principio di «minimizzazione dei dati», in violazione dell'art. 5, par. 1, lett. b) e c), del RGPD; - <u>non adottando «misure tecniche e organizzative» adeguate «ad attuare in modo efficace i principi di protezione dei dati» fin dalla progettazione</u> e per garantire che siano trattati per «impostazione predefinita» solo «i dati personali necessari per ogni specifica finalità del trattamento», in violazione dell'art. 25, parr. 1 e 2, del RGPD.
Sanzione: euro 5.000,00

Provvedimento Garante : n. 281 del 22/07/2021
Fattispecie : pubblicazione nell'Albo pretorio, nel Registro degli accessi e nella sezione "Amministrazione trasparente" del documento contenente – oltre i dati del professionista incaricato – incidentalmente anche i dati personali di un soggetto terzo estraneo alla dichiarazione , ossia il reclamante sig. XX (quali relativo nominativo, residenza e informazioni inerenti alla presentazione di un ricorso contro il comune per l'annullamento di un ordinanza sindacale di inagibilità);
Violazioni : l'illiceità del trattamento di dati personali effettuato dal Comune di, in quanto: 3) la diffusione dei dati personali del reclamante contenuti nel documento intitolato «XX» di un altro professionista, sopra identificato ..., è <u>in contrasto con il principio di «minimizzazione» dei dati</u> , che non risultano «limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (ossia la trasparenza dell'«attestazione dell'avvenuta verifica dell'insussistenza di situazioni, anche potenziali, di conflitto di interessi» del consulente/collaboratore dell'ente), in violazione dell'art. 5, par. 1, lett. c), del RGPD; 4) <u>la diffusione dei dati personali del reclamante e degli altri soggetti interessati che hanno inoltrato richieste di accesso al Comune</u> — contenuti nel documento, nonché nel «XX» presenti nella sezione Amministrazione trasparente, agli url indicati nelle lettere da a) ad h) del medesimo paragrafo — <u>risulta avvenuta in assenza di idonei presupposti normativi</u> , in violazione dell'art. 2-ter, commi 1 e 3, del Codice (e in maniera non conforme alle indicazioni contenute nelle Linee guida dell'ANAC e nella Circolare della funzione pubblica sopra richiamate al par. 2); nonché dei principi di base del trattamento contenuti negli artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD.
Sanzione: euro 2.200,00

RESPONSABILE PROTEZIONE DATI

Provvedimento Garante: n. 54 del 11/02/2021
Fattispecie: ritardata nomina del Responsabile della Protezione dei Dati (RPD) e della comunicazione al Garante dei relativi dati di contatto - pubblicazione di curriculum vitae con dati personali anche sensibili.
Violazioni accertate: non ha designato, essendovi tenuto, il Responsabile della Protezione dei Dati (RPD), né ha comunicato a questa a questa Autorità i relativi dati di contatto dopo averlo nominato, entro la data del 25/5/2018 in cui è divenuto applicabile il RGPD, avendo provveduto a tale adempimento solo a distanza di circa anno e mezzo e precisamente in data XX (per la nomina del RPD) e in data XX (per la comunicazione dei dati di contatto), in violazione dell'art. 37, parr 1 e 7, del RGPD.
Sanzione: euro 75.000,00 <i>[comprensiva della sanzione per la pubblicazione illecita di moltissimi curricula vitae di candidati manager per imprese private.]</i>

Provvedimento Garante n. 272 del 17/12/2020
Fattispecie: delibera GM, pubblicata nella sezione Amministrazione Trasparente e all'Albo pretorio, contenente una denuncia-querela da parte del Sindaco nei confronti di un consigliere comunale
Violazioni : <u>mancata designazione del «responsabile della protezione dei dati»; mancata pubblicazione e comunicazione al Garante dei relativi contatti, applicazione del RGPD, in violazione dell'art. 37, parr. 1, lett. a), e 7, del RGPD.</u>
Sanzione: euro 10.000

Provvedimento Garante n. 54 dell'11/02/2021
Fattispecie: all'url https://... era presente una pagina web intitolata « Elenco Manager » nella quale erano visibili e liberamente scaricabili dati personali (nominativo, codice fiscale, e-mail) e curriculum vitae integrale (con ulteriori dati personali come, ad esempio, telefono cellulare, istruzione e formazione, dettagliate esperienze professionali, in alcuni casi anche copia del documento di riconoscimento e della tessera sanitaria ecc.) riferiti a più di cinquemila <u>soggetti interessati</u> , inseriti nell'elenco dei «Manager qualificati e delle società di consulenza». Inoltre, all'url https://... era possibile scaricare l'allegato al decreto direttoriale del Ministero dello sviluppo economico del XX con cui è stato approvato il citato «elenco dei manager qualificati e delle società di consulenza istituito ai sensi del decreto ministeriale XX e formato sulla base dei dati e delle informazioni dichiarati dagli istanti», contenente dati e informazioni personali di tutti i predetti soggetti (fra cui nominativo, codice fiscale, e-mail).
Violazioni: <ul style="list-style-type: none"> ➤ per la pubblicazione on-line di dati personali : <ul style="list-style-type: none"> - <u>assenza di un idoneo presupposto normativo</u>, in violazione dell'art. 2-ter, commi 1 e 3, del Codice e dell'art. 6, par. 1, lett. c) ed e); par. 2 e par. 3, lett. b), del RGPD - mancato rispetto dei principi di "liceità", "limitazione della finalità" e "minimizzazione dei dati", in violazione dell'art. 5, par. 1, lett. a), b) e c), del RGPD; ➤ <u>ritardo nella nomina del Responsabile della Protezione dei Dati (RPD) del MISE, nonché della comunicazione a questa Autorità dei relativi dati di contatto</u>, entrambi avvenuti in data successiva al 25/5/2018 in cui è divenuto obbligatorio il RGPD, in violazione dell'art. 37, parr 1 e 7, del Regolamento europeo.
Sanzione: euro 75.000,00

RIFIUTI - RACCOLTA INDIFFERENZIATA

Provvedimento Garante: n. 1149822 del 14/07/2005
Con questo provvedimento il Garante ha diramato le proprie “prescrizioni” da osservare per la tutela dei dati personali da proteggere durante l'espletamento del servizio di raccolta differenziata dei rifiuti urbani interni “porta a porta” .
A garanzia degli interessati, il Garante prescrive a tutti i titolari del trattamento interessati , e in particolare a quelli oggetto dei reclami, quesiti e segnalazioni in atti, di conformare gli eventuali trattamenti di dati personali utilizzati ai seguenti principi in materia di protezione dei dati personali (art. 154, comma 1, lett. c) del Codice) , tenendo presenti anche gli obblighi che attengono: a) alla predisposizione dell'informativa (art. 13); b) alle misure di sicurezza (artt. 31-36 e allegato B)); c) all'individuazione dei brevi periodi di eventuale conservazione dei dati personali raccolti e alla selezione dei soggetti che, in qualità di incaricati o responsabili del trattamento, sono autorizzati a compiere operazioni di trattamento sulla base dei compiti assegnati e delle istruzioni impartite (artt. 29 e 30).
Principi : l' obbligo di utilizzare sacchetti trasparenti per conferire i rifiuti non è proporzionato al rischio che i dati personali anche di natura sanitaria, di quanti costituiscono il nucleo familiare del conferente, possano essere conosciuti non soltanto dagli operatori del servizio ma anche da parte di chiunque si trovi a transitare sul pianerottolo o, comunque, in prossimità dello spazio pubblico o privato su cui sono depositi i sacchetti; <ul style="list-style-type: none"> ▪ esporre sui contenitori - con etichette o targhette - il nome e il cognome dell'intestatario degli stessi contenitori con cui si conferiscono i rifiuti viola il predetto principio di proporzionalità; ▪ deve ritenersi lecito sia contrassegnare il sacchetto dei rifiuti mediante un codice a barre relativo ai dati identificativi del soggetto cui il contenitore si riferisce (anche se collegato ad un database anagrafico presso il Comune), sia fornire agli utenti appositi sacchetti dotati di microchip o, eventualmente, di dispositivi Radio Frequency Identification ("RFID"), da utilizzare obbligatoriamente per una determinata tipologia di materiale, e

ciò in quanto le descritte procedure consentono di delimitare l'identificabilità del conferente ai soli casi in cui sia stata accertata la mancata osservanza delle prescrizioni in ordine alla differenziazione. Al momento dell'apertura del sacchetto, i soggetti preposti alla verifica dell'omogeneità dei materiali inseriti, che comunque sono tenuti al rispetto della riservatezza, vengono, infatti, a conoscenza del contenuto, ma non anche, in prima battuta, degli elementi identificativi del soggetto conferente. Invece, i soggetti preposti all'applicazione della sanzione, mediante la decodifica del codice a barre o del microchip, acquisiscono il nominativo del soggetto cui il sacchetto si riferisce, solo in relazione alla non conformità del contenuto del sacchetto

- **Ispezione dei sacchetti.** Agli organi addetti al controllo è riconosciuta la possibilità di procedere a ispezioni di cose e luoghi diversi dalla privata dimora per accertare le violazioni di rispettiva competenza (art. 13, l. 24 novembre 1981, n. 689). Tale facoltà deve essere esercitata selettivamente, nei soli casi in cui il soggetto che abbia conferito i rifiuti con modalità difformi da quelle consentite non sia in altro modo identificabile. Risulterebbe, quindi, invasiva la pratica di ispezioni generalizzate da parte del personale incaricato (agenti di polizia municipale; dipendenti di aziende municipalizzate), del contenuto dei sacchetti al fine di trovare elementi informativi in grado di identificare, presuntivamente, il conferente. Qualora siano utilizzati sacchetti dotati di microchip, di codici a barre o, eventualmente, di "RFID", non è quindi necessario procedere ad ispezioni al fine di individuare il conferente. La modalità di accertamento descritta può poi rivelarsi lesiva di situazioni giuridicamente tutelate come la libertà e la segretezza della corrispondenza lasciata nei rifiuti. L'attività di ispezione non costituisce, peraltro, strumento di per sé risolutivo per accertare l'identità del soggetto produttore, dal momento che non sempre risulta agevole provare che il medesimo sacchetto, avente un contenuto difforme da quello per il quale il sacchetto è utilizzabile, provenga proprio dalla persona individuata mediante una ricerca di elementi presenti nel medesimo. Tale considerazione induce a ritenere che il trasgressore non dovrebbe essere individuato sempre ed esclusivamente attraverso una ricerca nel sacchetto dei rifiuti di elementi (corrispondenza o altri documenti) a lui riconducibili, e che quindi una eventuale sanzione amministrativa irrogata ad un soggetto così individuato potrebbe risultare erroneamente comminata. Alle stesse conclusioni si deve pervenire nella diversa ipotesi in cui la violazione consista nel mancato rispetto dell'orario di conferimento.
- **Ecopiazze.** La richiamata procedura prevede una registrazione, da parte dei soggetti preposti alla gestione di apposite aree per il conferimento organizzato dei materiali della raccolta differenziata, del nome e dell'indirizzo dei conferenti i materiali della raccolta differenziata (previa esibizione di un documento di identità), nonché della quantità approssimativa e del tipo di materiale ricevuto. Alcuni regolamenti comunali prevedono che, nei limiti di una quantità massima giornaliera indicata nel regolamento stesso, in relazione alle diverse tipologie di materiali, i rifiuti siano conferiti senza oneri da parte dei produttori. Nel caso in cui siano superate le quantità indicate per ogni tipologia di rifiuto, il produttore ricorre alla raccolta a domicilio, contattando la società di gestione del servizio, previo pagamento delle spese. In relazione a tale aspetto, deve ritenersi lecito, nei limiti dello svolgimento delle finalità istituzionali sopra descritte e ove sia previsto da una disposizione regolamentare (cfr. art. 21 del d.lg. n. 21/1997), il trattamento dei dati personali (es.: nome e indirizzo dei conferenti), per la sola finalità di accertamento dell'effettiva residenza nel comune del conferente e per evitare che lo stesso soggetto possa conferire i rifiuti in violazione dei limiti quantitativi ammessi senza oneri a carico dei produttori. Deve essere comunque predisposta un'informativa contenente gli elementi indicati nell'art. 13 del Codice e i dati personali acquisiti devono essere conservati per il solo periodo necessario allo scopo per i quali essi sono stati raccolti (art. 11, comma 1, lett. d)).

SERVIZI ESTERNALIZZATI

Provvedimento Garante n. 280 del 17/12/2020

Fattispecie: illiceità del trattamento dei dati personali di utenti e dipendenti effettuato dal Comune di mediante un **sistema informatico**, fornito da s.r.l. (di seguito, la "Società"), utilizzato, fin dal 2015, **per finalità di prenotazione degli appuntamenti e di erogazione dei servizi di sportello.**

Violazioni:

il trattamento è stato effettuato in contrasto:

- con i principi di liceità, correttezza e trasparenza (artt. 5, par. 1, lett. a) e con l'obbligo, posto in capo al titolare del trattamento, di fornire l'informativa agli utenti e ai dipendenti (artt. 13 e 14 del Regolamento, già art. 13 del Codice, anteriormente alle modifiche di cui al d.lg. n.101/2018);
- con l'obbligo di regolamentare, con un atto avente le caratteristiche di cui all'art. 28, paragrafi 2 e 3 del Regolamento (già art. 29 del Codice, anteriormente alle modifiche di cui al d.lgs. n.101/2018), i trattamenti di dati personali affidati, per conto del titolare, alla Società nell'ambito dei servizi di assistenza e manutenzione del sistema informatico;

- con l'obbligo di adottare misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, tenendo conto, in particolare, della natura, dell'oggetto, del contesto, delle finalità e dei rischi inerenti al trattamento per i diritti e le libertà delle persone fisiche (art. 32 del Regolamento)

Sanzione: euro 500.000,00

Provvedimento Garante n. 281 del 17/12/2020

Fattispecie: esternalizzazione del **programma informatico per finalità di prenotazione da parte di cittadini e dipendenti comunali degli appuntamenti e di erogazione dei servizi di sportello;**

Violazioni:

illecito trattamento di dati personali effettuato dalla Società fornitrice e gestore, per conto del Comune affidatario, del programma informatico, in violazione:

- dei principi di base del trattamento;
- in assenza di idonea base giuridica per il trattamento di dati personali di utenti e dipendenti del Comune enti a cui è stata fornita la piattaforma "....i";
- senza aver regolamentato il rapporto con i c.d. "Agenti di prenotazione", cc.dd. broker, in violazione degli artt. 5, par. 1, lett. a) ed e), 6, 9 e 28 del Regolamento.

Sanzione: euro 40.000,00

Provvedimento Garante n. 294 del 22/07/2021

Fattispecie: il Comune di ha affidato alla propria società ZZZ i **servizi complementari al trasporto pubblico di linea, relativi alla gestione dei parcheggi di scambio e della sosta tariffata su strada**, di competenza del Comune; alcuni **parcometri in gestione** sono stati oggetto di adeguamento tecnologico, al fine di consentire il pagamento anche mediante carte di debito/credito, la personalizzazione del pagamento mediante l'inserimento della targa del veicolo (con la conseguente non necessità per l'utente di esporre il tagliando di pagamento) e la possibile attivazione di servizi aggiuntivi sul parcometro (es. pagamento sanzione/tributi, acquisto/rinnovo dei titoli del trasporto pubblico);

Per quanto riguarda l'architettura funzionale del sistema, Atac s.p.a ha realizzato un sistema centralizzato che si occupa di raccogliere le informazioni (l'ora, la data di inizio e fine sosta, l'importo pagato e la targa) relative al pagamento della sosta effettuato tramite app messe a disposizione da diversi gestori (myCicero, easyPark, etc.) o parcometri "evoluti" Pay&Go (gestiti dalla società Parkeon s.r.l., ora Flowbird Italia s.r.l.) e di renderle disponibili sia agli ausiliari al traffico per le finalità di verifica dell'avvenuto pagamento della sosta (mediante l'utilizzo dell'app E-Multe-S, installata sugli smartphone aziendali), sia al personale interno della società per finalità di gestione amministrativa.

Violazioni: Il Comune di non ha provveduto a nominare la propria società ZZZ quale responsabile del trattamento in violazione dei principi generali del trattamento; assenza di idonea informativa; assenza della nomina dei responsabili del trattamento; assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio presentato dal trattamento; violazione degli artt. 5, 12, 13, 25, 28 e 32 del RGDP.

E' stato accertato:

- che la società ZZZ non aveva provveduto a implementare misure per la cancellazione dei dati né adottate misure tecniche idonee alla conservazione dei dati personali, in forma anonima o pseudonima.
- alcuni flussi di dati "da e verso" il sistema ATAC non si avvalgono di canali di comunicazioni sicuri;
- il sistema di autenticazione non garantisce idonee misure di sicurezza relativamente al formato delle password ed alla memorizzazione delle stesse nel database;
- non risulta implementato alcun meccanismo che consenta la tracciabilità delle operazioni effettuate (log applicativo) dagli utenti del sistema sui dati personali, siano essi amministratori di sistema ovvero operatori di back office e ausiliari al traffico;

Il trattamento risulta essere stato effettuato dal Comune di in violazione dell'obbligo che impone al titolare del trattamento di rendere agli interessati una preventiva informativa, secondo quanto previsto dagli artt. 12 e 13 del Regolamento, anche nel rispetto del "principio di trasparenza" (art. 5, lett. a) del Regolamento).

Il titolare del trattamento non ha messo "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 la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità" (art 25, par. 1 e 2) e non ha definito i tempi di conservazione dei dati personali raccolti né ha dato in tal senso precise istruzioni a ZZZ s.p.a. di cui agli artt. 5, par. 1, lett. e) e 25 e del Regolamento.

Sanzione: euro 800.000,00

Provvedimento Garante n. 293 del 22/07/2021
Fattispecie: servizio parcometri gestito dalla società in house del Comune (vedi GP 294-2021)
Violazioni: <u>assenza di una condizione di liceità; mancanza di adempimento dell'obbligo di redigere un registro del trattamento; assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio presentato dal trattamento; violazione degli artt. 5 par. 1 lett. a), 6, 30 e 32 del Regolamento.</u>
Sanzione: euro 400.000,00 comminata alla società in house

Provvedimento Garante n. 9 del 14/01/2021
Fattispecie: gestione delle prenotazioni delle prestazioni sanitarie, attraverso il call center regionale (ReCUP). Il Garante ha ribadito che le società che prestano servizi per conto del titolare e che di conseguenza trattano i dati personali degli utenti, devono essere designate responsabili del trattamento. Il rapporto tra titolare e responsabile deve essere regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, prevede nel dettaglio le regole e i limiti con cui devono essere trattati i dati personali. Il responsabile è, pertanto, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare". L'Edpb, il Comitato che riunisce le Autorità di protezione dati dell'Ue, ha affermato che l'assenza di una chiara definizione del rapporto tra titolare e responsabile può sollevare il problema della mancanza di base giuridica su cui ogni trattamento deve fondarsi: ad esempio, per quanto riguarda la comunicazione dei dati tra titolare e responsabile. La designazione del Responsabile del trattamento da parte della Società, controllata dalla Regione, è "ritenuta priva di effetti", in quanto la designazione sarebbe dovuta essere stata effettuata dal titolare del trattamento, cioè dalla Regione.
Violazioni: per il ritardo nella nomina del Responsabile della Protezione dei Dati (RPD) in violazione dell'art. 37, parr 1 e 7, del Regolamento europeo
Sanzione: euro 75.000,00

STRUMENTI - PROGRAMMI INFORMATICI

Provvedimento Garante: n. 399 del 28/06/2018
Fattispecie: la Guardia di finanza, Nucleo speciale privacy ha accertato, nei confronti di ASL le seguenti condotte illecite: diversi applicativi informatici in uso presso il presidio, è emerso che <u>le credenziali per l'accesso ad alcuni di essi (Hdgold Olivetti, Hospital Cardio, Geos, Gepadial, Armonia, Emodata) sono condivise fra i dipendenti che li utilizzano.</u> E' inoltre emerso che, con riferimento a due sistemi (Hospital Cardio e Edotto Sist), alcuni dipendenti vi accedono utilizzando password composte da meno di otto caratteri alfanumerici;
Violazioni accertate: l'Asl, sulla base delle considerazioni sopra richiamate, risulta aver commesso la violazione prevista dall'art. 162, comma 2-bis, del Codice, <u>per aver omesso di adottare le misure minime di sicurezza previste dagli artt. 33 e ss. del Codice e dalle regole nn. 3, 4, 5 e 6 del disciplinare tecnico di cui all'allegato B) del medesimo Codice.</u>
Sanzione: euro 20.000,00

TRATTAMENTO SANITARIO OBBLIGATORIO

Provvedimento Garante n. 68 del 05/02/2015
Fattispecie: ordinanza sindacale con cui si dispone un TSO
Violazioni: illecita, per contrasto con il disposto dell'art. 22, comma 8, del Codice, la pubblicazione sul sito istituzionale di un ente locale di una ordinanza che contenga dati relativi alle condizioni di salute. (Nel caso di specie si trattava di una ordinanza sindacale con cui veniva disposto un ricovero urgente per trattamento sanitario obbligatorio [TSO], con espressa indicazione dei dati anagrafici e di salute relativi all'interessato).
Sanzione: euro 10.000,00

VARIE

Parere Garante: newsletter del 21/05/2020
Fattispecie: qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza (di seguito, OdV)
parere : <ul style="list-style-type: none">- l'OdV, pur essendo dotato di autonomi poteri di iniziativa e controllo, non possa essere considerato autonomo titolare del trattamento (art. 4, n. 7 del Regolamento), considerato che i compiti di iniziativa e controllo propri dell'OdV non sono determinati dall'organismo stesso, bensì dalla legge che ne indica i compiti e dall'organo dirigente che nel modello di organizzazione e gestione definisce gli aspetti relativi al funzionamento compresa l'attribuzione delle risorse, i mezzi e le misure di sicurezza (art. 6, commi 1 e 2 d.lgs. n. 231/2001).- l'OdV non ha l'obbligo di denuncia all'Autorità giudiziaria in relazione agli illeciti di cui viene a conoscenza a causa e nell'esercizio delle sue funzioni (obbligo che grava invece sull'ente all'uopo informato dall'OdV) né è l'organismo investito di poteri disciplinari nei confronti degli autori degli illeciti, poteri che rimangono in capo all'ente ai cui vertici aziendali l'OdV è tenuto a segnalare le violazioni accertate, proponendo, al contempo, l'adozione delle necessarie sanzioni.- tenuto conto che l'OdV non è distinto dall'ente, ma è parte dello stesso, si ritiene che - valutate anche le attribuzioni e le caratteristiche indicate nell'art. 6, d.lgs. n.231/2001 - non possa essere considerato responsabile del trattamento inteso come soggetto chiamato ad effettuare un trattamento "per conto del titolare", ovvero sia una "persona giuridicamente distinta dal Titolare, ma che agisce per conto di quest'ultimo" secondo le istruzioni impartite dal titolare (art. 28 del Regolamento). <p>si ritiene che l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongano siano interni o esterni, debba essere considerato "parte dell'ente". Il suo ruolo - che si esplica nell'esercizio dei compiti che gli sono attribuiti dalla legge, attraverso il riconoscimento di "autonomi poteri di iniziativa e controllo" - si svolge nell'ambito dell'organizzazione dell'ente, titolare del trattamento, che, attraverso la predisposizione dei modelli di organizzazione e di gestione, definisce il perimetro e le modalità di esercizio di tali compiti. Tale posizione si intende ricoperta dall'OdV nella sua collegialità, tuttavia, non può prescindere dalla necessità di definire anche il ruolo che, in base alla disciplina in materia di protezione dei dati personali, deve essere previsto per i singoli membri che lo compongono. Lo stesso ente, in ragione del trattamento dei dati personali che l'esercizio dei compiti e delle funzioni affidate all'OdV comporta (ad esempio, l'accesso alle informazioni acquisite attraverso flussi informativi), designerà - nell'ambito delle misure tecniche e organizzative da porre in essere in linea con il principio di accountability (art. 24 del Regolamento) - i singoli membri dell'OdV quali soggetti autorizzati (artt. 4, n. 10, 29, 32 par. 4 Regolamento; v. anche art. 2-quaterdecies del Codice). Tali soggetti dovranno attenersi alle istruzioni impartite dal titolare affinché il trattamento avvenga in conformità ai principi stabiliti dall'art. 5 del Regolamento.</p>

Provvedimento Garante n. 280 del 22/07/2021
Fattispecie: decreto dirigenziale di revoca di un finanziamento concesso a una ditta pubblicato sul sito web
Violazioni: <ul style="list-style-type: none">➤ diffusione online di dati e informazioni personali del reclamante (quali il nominativo e l'indirizzo di residenza), contenuti nel testo e nell'oggetto del decreto dirigenziale "non limitati alla finalità del trattamento" in violazione del principio di "minimizzazione" dei dati ex art. 5, prf. 1, lett. c) RGDP➤ <u>assenza di idoneo presupposto normativo</u> in violazione dell'art. 2-ter, commi 1 e 3, del Codice➤ <u>violazione dei principi di base del trattamento</u> ex artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD
Sanzione: euro 10.000,00

Provvedimento Garante n. 116 del 02/07/2020
Fattispecie: la sig.ra XX, dipendente del Comune di, ha lamentato la comunicazione di propri dati personali, attraverso l'invio di "una nota stampa", da parte della Commissione Straordinaria del Comune, a "due testate giornalistiche locali e a due di rilievo regionale" , nella quale la reclamante veniva menzionata "con riferimento all'attivazione di una procedura stragiudiziale [...] per il riconoscimento di mansioni superiori". Secondo il titolare del trattamento [il Comune] il comunicato stampa (contenente i dati, riferibili anche a vicende penali e a misure di sicurezza e prevenzione, di cinque persone, tra cui tre testimoni citati a comparire) è stato inviato nell'esercizio del diritto di cronaca ad alcune testate locali al fine di tutelare l'immagine dell'Amministrazione.
Violazioni: aver comunicato a terzi dati personali relativi alla reclamante, in <u>assenza di idonei presupposti normativi</u> , in violazione dell'art. 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGDP e dell'art. 2-ter del Codice.
Sanzione: euro 2.000,00

Provvedimento Garante n. 206 del 13/05/2021
Fattispecie: questionario inviato tramite tre mail con indirizzi multipli inseriti nel campo (...) Cc, anziché nel campo (...) Ccr/Ccn, consentendo ai destinatari delle mail di conoscere gli indirizzi di posta elettronica degli altri 61 destinatari della comunicazione e magari risalire all'identità degli altri destinatari e ai relativi dati attenenti alla salute.
Violazioni: illecita comunicazione di dati personali sulla salute che possono essere comunicate solo all'interessato e possono essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o su indicazione dello stesso interessato previa delega scritta di quest'ultimo ex art. 9 RGDP e art. 83 Codice
Sanzione: euro 20.000,00

Provvedimento Garante n. 197 del 13/05/2021
Fattispecie: sulla pagina Facebook "XXX Sindaco di XXX" sono stati pubblicati dati personali, spesso contenuti in video e immagini, di soggetti descritti quali autori o presunti autori di infrazioni, esponendo in tal modo i medesimi a commenti lesivi della loro dignità formulati da parte degli utenti del social network. Tale condotta è stata posta in essere senza peraltro garantire alcuna tutela nei confronti delle categorie più fragili, quali minori e persone in condizione di difficoltà sociale ed economica, come dimostra l'avvenuta diffusione, tra gli altri, di un video ritraente persone, ivi inclusa una presumibilmente minore di età, colte nell'atto di gettare rifiuti ingombranti in un'area non deputata allo smaltimento degli stessi o di quello contenente immagini di cittadini extraeuropei senza fissa dimora ripresi, nelle prime ore del mattino, sdraiati in terra all'interno di un edificio pubblico. Il soggetto titolare dell'account utilizzato per la diffusione dei contenuti indicati è XXX, che ha dichiarato che l'acquisizione dei "contenuti è avvenuta su strada pubblica da parte di un privato cittadino attraverso l'utilizzo di uno smartphone che, inviando in forma privata al Sindaco, ha inteso, attraverso il video, riprendere la condotta di chi in quel momento stava consumando un reato ambientale, in una delle strade urbane più trafficate della città, incurante peraltro del rischio di essere colto in flagranza, al fine di denunciare al Sindaco, quindi ad una pubblica autorità"
Violazioni: il trattamento non è apparso sorretto dalla base giuridica richiesta dalle norme, né comunque disciplinato da atti interni dell'ente diretti a contemplare l'utilizzo dei social network nell'ambito del perseguimento di finalità connesse all'esercizio di compiti di interesse pubblico; il trattamento effettuato non può essere inequivocabilmente ricondotto alla titolarità dell'ente [Comune] rappresentato, ma appare per lo più quale espressione di un'iniziativa del singolo.
Sanzione: euro 50.000,00

VIDEO SORVEGLIANZA

Provvedimento Garante n. 132 del 05/03/2015
Fattispecie: informativa sintetica (di primo livello)
Violazioni: mancata informativa sui dati raccolti attraverso l'impianto di video sorveglianza e insufficiente informativa sintetica in proporzione all'estensione (250 ettari) del resort.
Sanzione: euro 18.000,00

Provvedimento Garante n. 183 del 15/10/2020
Fattispecie: istanza per l'esercizio di accesso ai propri dati personali a seguito di un verbale di accertamento di violazione al codice della strada rilevata con sistema di videosorveglianza.
Violazioni: ritardato (dopo quasi un anno) riscontro all'istanza di accesso violando il termine di 30 giorni previsto dall'art. 12 del RGDP, senza, peraltro, aver informato il reclamante dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale entro il medesimo termine
Sanzione: euro 2.000,00

Parere Garante: n. 20 del 27/01/2022
Fattispecie: Con la nota del xxx, la Polizia Municipale del Comune di comunicava a questa Autorità di aver effettuato, in data xxx, un'ispezione presso il circolo privato "....." (di seguito il "Circolo"), sito a, via n. ..., a seguito di una segnalazione della Stazione dei Carabinieri di Dalle attività ispettive svolte dal Reparto Sicurezza Urbana e Patrimonio veniva accertato che, presso il Circolo, era funzionante un impianto di videosorveglianza non conforme alle norme in materia di protezione dei dati personali. In particolare, gli agenti appuravano che le telecamere, sei poste all'interno del locale e tre all'esterno e collegate a un sistema informatico interno

all'immobile non erano segnalate da alcun cartello contenente l'informativa e che due delle telecamere esterne presentavano un angolo di visuale orientato verso il marciapiede e la carreggiata di fronte al Circolo, con inquadratura rivolta, in un caso, anche verso la facciata della Caserma della Stazione dei Carabinieri prossima alla sede del circolo.

L'Ufficio, sulla base delle risultanze degli accertamenti eseguiti, provvedeva a notificare al Circolo (prot. n.) l'atto di avvio del procedimento sanzionatorio, ai sensi dell'art. 166, comma 5, del Codice in relazione alla violazione dell'art. 5, par. 1, lett. a) e c) del Regolamento (angolo di visuale non circoscritto all'area del Circolo) e dell'art. 13 del Regolamento (assenza dell'informativa).

La parte non inviava memorie o scritti difensivi (art. 18 della legge n. 689/1981).

Violazioni accertate: L'utilizzo di sistemi di videosorveglianza può determinare, in relazione al posizionamento delle telecamere e alla qualità delle immagini riprese, un trattamento di dati personali. Tale trattamento deve essere effettuato nel rispetto dei principi generali contenuti nell'art. 5 del Regolamento e, in particolare, del principio di trasparenza che presuppone che "gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata".

A questo scopo quindi il titolare del trattamento deve apporre **idonei cartelli informativi** secondo le indicazioni contenute al punto 3.1. del provvedimento in materia di videosorveglianza - 8 aprile 2010 [1712680] (in tal senso anche le Faq in materia di videosorveglianza, pubblicate sul sito web dell'Autorità).

Analogamente le Linee Guida n. 3/2019 del Comitato europeo per la protezione dei dati sul trattamento dei dati personali attraverso dispositivi video, punto 7) specificano che "Per quanto riguarda la videosorveglianza, le informazioni più importanti devono essere indicate [dal titolare] sul segnale di avvertimento stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello). Nelle linee guida si prevede inoltre che "Tali informazioni possono essere fornite in combinazione con **un'icona per dare, in modo ben visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto** (articolo 12, paragrafo 7, del RGPD). Il formato delle informazioni dovrà adeguarsi alle varie ubicazioni". Le informazioni dovrebbero essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, **prima di entrare nella zona sorvegliata** (approssimativamente all'altezza degli occhi) "per consentire all'interessato di stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario".

Occorre poi considerare che la necessità di utilizzare la videosorveglianza a protezione degli interessi legittimi di un titolare si arresta ai confini delle aree di propria pertinenza. Anche **nei casi in cui si renda necessario estendere la videosorveglianza alle immediate vicinanze dell'area di pertinenza, il titolare del trattamento deve comunque mettere in atto misure idonee a evitare che il sistema di videosorveglianza raccolga dati anche oltre le aree di pertinenza, eventualmente oscurando tali aree** (vedi in proposito Linee Guida n. 3/2019 del Comitato europeo per la protezione dei dati sul trattamento dei dati personali attraverso dispositivi video, punto 27).

Risulta accertato che **il Circolo ha effettuato un trattamento di dati personali, per mezzo di un impianto di videosorveglianza in violazione dei principi generali in materia di protezione dei dati personali** di cui all'art. 5, par. 1, lett. a) e c) e **in assenza di idonea informativa** in spregio a quanto stabilito dall'art. 13 del Regolamento.

risulta accertato che il Circolo ha effettuato un trattamento di dati personali, per mezzo di un impianto di videosorveglianza in violazione dei principi generali in materia di protezione dei dati personali di cui all'art. 5, par. 1, lett. a) e c) e in assenza di idonea informativa in spregio a quanto stabilito dall'art. 13 del Regolamento.

Sanzione: euro 2.000,00

Provvedimento Garante: n. 162 del 28/04/2022

Fattispecie: la società XXX s.p.a. (di seguito, la società), gestore del **servizio di raccolta dei rifiuti urbani** per il Comune di ZZZ (di seguito, il Comune), ha installato alcune **videocamere allo scopo di individuare e sanzionare comportamenti illegali.**

Da quanto risulta documentato nella segnalazione, la società avrebbe diffuso, attraverso la pubblicazione nel proprio profilo Facebook, alcuni video e alcune immagini, raccolte attraverso i sistemi di videosorveglianza installati sul territorio comunale, dalle quali risulterebbero identificabili alcuni soggetti interessati.

Modalità di espletamento della videosorveglianza:

la società ha dichiarato che:

"Con Ordinanza Sindacale n. ... del è stato disposto [...] il conferimento al personale [della società], totalmente partecipata [dal Comune], delle funzioni di accertamento e contestazione immediata degli illeciti amministrativi derivanti dalla violazione delle norme regolamentari comunali sullo smaltimento dei rifiuti [...]";

"dato il dilagante fenomeno dell'abbandono dei rifiuti, al fine di contenere questi atti di inciviltà, l'Amministrazione del Comune [...] e [...] la società, hanno condiviso la volontà di installare nei siti più sensibili, dove gli abbandoni si ripetono, dei sistemi di videosorveglianza/fototrappole";

"il Comune [...] con Decreto Sindacale Prot. [...] del XX, ha conferito l'incarico di ausiliari ecologici a dei Dipendenti [...]

della società”;

“in tale Decreto, sono indicate anche le modalità di trasmissione degli illeciti: ‘trasmetterà i verbali di accertamento delle infrazioni, con irrogazione della sanzione, alla Direzione Polizia Locale di Taranto che curerà i conseguenziali adempimenti relativi alla verifica del pagamento in misura ridotta ovvero all’attivazione del procedimento ex art 18 L.n. 689/81 [...]”.

In allegato a tale nota la società ha fornito un modello di verbale di accertamento di illecito amministrativo redatto su carta cointestata della società e del corpo di polizia locale del Comune, nel quale esplicitamente si fa riferimento alla circostanza che “l’accertamento è stato rilevato mediante immagini registrate da apposita telecamera di videosorveglianza mobile [...]” (all. 4), un esempio di cartello informativo che rilevarebbe la presenza di una telecamera (all. 6); nonché alcune immagini pubblicate sul profilo Facebook della società (all. 7).

Violazioni: l’Ufficio ha rilevato che il Comune ha posto in essere, per il tramite della società, un trattamento dei dati personali dei cittadini attraverso un sistema di videosorveglianza:

- in assenza di idonea informativa, che deve essere conferita “nel momento in cui i dati personali sono ottenuti”, con conseguente violazione del principio di “liceità, correttezza e trasparenza”, di cui all’art. 5, par. 1, lett. a) del Regolamento e degli artt. 12, 13 e 14 del Regolamento;
- in mancanza di idonea disciplina del rapporto con la società quale “responsabile del trattamento”, prima dell’inizio del trattamento stesso, in violazione dell’art. 28 del Regolamento (già art. 29 del Codice previgente);
- in assenza di valutazione di impatto, in violazione dell’art. 35 del Regolamento.

Sanzione: euro 150.000,00

Provvedimento Garante: n. 163 del 28/04/2022

Fattispecie: la società XXX s.p.a.(di seguito, la società), gestore del **servizio di raccolta dei rifiuti urbani** per il Comune di (di seguito, il Comune), ha installato alcune **videocamere allo scopo di individuare e sanzionare comportamenti illegali**.

Da quanto risulta documentato nella segnalazione, la società avrebbe diffuso, attraverso la pubblicazione nel proprio profilo Facebook, alcuni video e alcune immagini, raccolte attraverso i sistemi di videosorveglianza installati sul territorio comunale, dalle quali risulterebbero identificabili alcuni soggetti interessati.

Modalità di espletamento della videosorveglianza:

la società ha dichiarato che:

“Con Ordinanza Sindacale n. ... del è stato disposto [...] il conferimento al personale [della società], totalmente partecipata [dal Comune], delle funzioni di accertamento e contestazione immediata degli illeciti amministrativi derivanti dalla violazione delle norme regolamentari comunali sullo smaltimento dei rifiuti [...]”;

“dato il dilagante fenomeno dell’abbandono dei rifiuti, al fine di contenere questi atti di inciviltà, l’Amministrazione del Comune [...] e [...] la società], hanno condiviso la volontà di installare nei siti più sensibili, dove gli abbandoni si ripetono, dei sistemi di videosorveglianza/fototrappole”;

“il Comune [...] con Decreto Sindacale Prot. [...] del ..., ha conferito l’incarico di ausiliari ecologici a dei Dipendenti [...] della società”;

“in tale Decreto, sono indicate anche le modalità di trasmissione degli illeciti: ‘trasmetterà i verbali di accertamento delle infrazioni, con irrogazione della sanzione, alla Direzione Polizia Locale di Taranto che curerà i conseguenziali adempimenti relativi alla verifica del pagamento in misura ridotta ovvero all’attivazione del procedimento ex art 18 L.n. 689/81 [...]”.

In allegato a tale nota la società ha fornito un modello di verbale di accertamento di illecito amministrativo redatto su carta cointestata della società e del corpo di polizia locale del Comune, nel quale esplicitamente si fa riferimento alla circostanza che “l’accertamento è stato rilevato mediante immagini registrate da apposita telecamera di videosorveglianza mobile [...]” (all. 4), un esempio di cartello informativo che rilevarebbe la presenza di una telecamera (all. 6); nonché alcune immagini pubblicate sul profilo Facebook della società (all. 7).

Violazioni: l’Ufficio ha rilevato che il Comune ha posto in essere, per il tramite della società, un trattamento dei dati personali dei cittadini attraverso un sistema di videosorveglianza in assenza :

- il trattamento dei dati in esame, svolto dalla società per conto del Comune (nei cui confronti è contestualmente adottato uno specifico provvedimento [provv. GP 162/2022]), è stato avviato senza che il ruolo fosse disciplinato ai sensi dell’art. 28 del Regolamento (né ai sensi dell’art. 29 del Codice previgente), in quanto l’ordinanza sindacale del 28 marzo 2012 con la quale sono state conferite, al personale della società, le funzioni di accertamento e contestazione degli illeciti amministrativi derivanti dalla violazione delle norme regolamentari comunali sullo smaltimento dei rifiuti, non soddisfa le caratteristiche dell’atto giuridico volto a regolamentare il rapporto con il Responsabile, non contenendo né gli elementi previsti dall’art. 29 del Codice previgente né gli elementi previsti dall’art. 28 del Regolamento.
- la società si è rivolta, nel mese di novembre 2020, alla società YYY s.r.l., fornitrice del sistema di

videosorveglianza (provvedendo a designarla quale “responsabile del trattamento”) senza la “previa autorizzazione scritta, specifica o generale, del titolare del trattamento” in violazione dell’art. 28, par. 2 del Regolamento.

- dagli atti, non risulta indicata la base giuridica che avrebbe legittimato la diffusione dei dati personali,
- risulta accertata la violazione del principio di “liceità, correttezza e trasparenza” (art. 5, par. 1 lett. a) del Regolamento);
- l’assenza di idonea base giuridica di cui agli artt. 6 del Regolamento e art. 2-ter del Codice (nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139, vigente al tempo dei fatti oggetto di segnalazione).
- non risultano forniti elementi che dimostrino la compatibilità dell’ulteriore trattamento (pubblicazione su Facebook) con le finalità in base alle quali i dati sono stati precedentemente raccolti e trattati, con conseguente violazione del principio di “limitazione della finalità” di cui all’art. 5 par. 1, lett. b) del Regolamento.

Sanzione: euro 200.000,00

ZONE A TRAFFICO LIMITATO

Provvedimento Garante n. 48 dell’11/02/2021

Fattispecie: i permessi per l’accesso e la sosta nelle zone a traffico limitato (“Z.T.L.”), da esporre sui veicoli, riportano sul frontespizio un **c.d. QR code**, che consente a chiunque, mediante l’utilizzo di una generica applicazione per dispositivi mobili (mobile app) in grado di decodificarne il contenuto, di accedere a dati personali relativi al titolare del permesso Z.T.L. o al suo utilizzatore; e, addirittura, anche ad altri titolari di permesso Z.T.L.;

le informazioni riportate “in chiaro” (non codificate nel QR code) sul contrassegno riguardano: la tipologia di autorizzazione (es. accesso, sosta, scarico merci, etc.), la targa del veicolo, il numero del permesso e la validità temporale; nel QR code sono invece riportate: la categoria del richiedente (es. domiciliato, distributore di merci, proprietario di posto auto, etc.), la ragione o denominazione sociale o istituzionale (in caso di veicolo appartenente a persona giuridica) o il nome e cognome (in caso di persona fisica) del titolare del permesso, nonché il nome e cognome dell’utilizzatore dello stesso;

Violazioni: illecito trattamento di dati personali effettuato, in quanto esso è avvenuto in maniera non conforme ai principi generali del trattamento, in assenza di un’idonea base giuridica, nonché in assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, in violazione dell’art. 32 del RGDP.

Sanzione: euro 60.000,00

Provvedimento Garante n. 49 dell’11/02/2021

Fattispecie: il Comune svolge attraverso una propria società la gestione dei permessi per l’accesso e la sosta nelle zone a traffico limitato (“Z.T.L.”);

i permessi riportano sul frontespizio un **c.d. QR code**, che consente a chiunque, mediante l’utilizzo di una generica applicazione per dispositivi mobili (mobile app) in grado di decodificarne il contenuto, di accedere a dati personali relativi al titolare del permesso Z.T.L. o al suo utilizzatore, tra cui: la denominazione sociale o istituzionale (es. Questura, scuola elementare) oppure il nome e il cognome (nel caso di persona fisica) del titolare del permesso, il nome e il cognome dell’utilizzatore del permesso, la categoria del richiedente (es. artigiano, lavoratore orari notturni), nonché la targa del veicolo autorizzato.

Ciò accadeva in quanto il servizio online di verifica dei permessi Z.T.L. risultava liberamente accessibile, non essendo protetto da alcuna procedura di autenticazione.

Inoltre, il Comune ha affidato alla propria società il servizio di hosting e di manutenzione di data base e connettività, la quale società ha trattato “dati personali” (art. 4, par. 1, n. 1), del Regolamento), effettuandone la registrazione e la conservazione.

Violazioni:

la diffusione dei predetti dati personali, a partire dal 1° dicembre 2016 (data a decorrere dalla quale è operativo, per i permessi Z.T.L, il formato cartaceo riportante un QR code e il relativo servizio online di verifica), è avvenuta in maniera non conforme ai principi di base di protezione dei dati, nonché in assenza di un idoneo presupposto normativo, in violazione degli artt. 5 e 6 del Regolamento e dell’art. 2-ter del Codice.

Sulla base degli elementi sopra riportati, deve quindi ritenersi che le operazioni sopra descritte diano luogo a un trattamento di dati personali da parte di ZZZ (cfr. “Guidelines 7/2020 on the concepts of controller and processor in the GDPR”, adottate dal Comitato europeo per la protezione dei dati il 2 settembre 2020, nella versione sottoposta a consultazione pubblica, in particolare, par. 2.1.4, punto 38, nella parte in cui è riportato l’esempio relativo agli “hosting services”), e che, pertanto, il ricorso da parte del Comune di ai servizi offerti da ZZZ – in

assenza di un contratto o altro atto giuridico che disciplinasse il trattamento di dati personali da parte di ZZZ, quale responsabile del trattamento – sia avvenuto in violazione dell'art. 28 del Regolamento.

Sanzione: euro 350.000,00