MULTIBUSINESS s.r.l.

Circolare del 07 dicembre 2020

INDICE

BUONI SPESA DEL COMUNE E RICHIESTA DI ACCESSO AGLI ATTI DA PARTE DI UN CONSIGLIERE COMUNALE

MINISTERO DELL'INTERNO: **è ammissibile** la richiesta del consigliere degli elenchi relativi ai percettori di contributi erogati dal comune per l'emergenza Covid-19

Con parere del 25 settembre 2020 (https://dait.interno.gov.it/pareri/98571), il Dip. Affari Interni del Viminale, in merito al diritto di accesso agli atti preteso da un consigliere comunale ai sensi dell'art. 43[1] del TUEL (D.Lgs. 267/2000 e ss.mm.ii.), ha ricordato che il diritto di accesso dei consiglieri comunali ha una ratio diversa da quella che contraddistingue il diritto di accesso dei cittadini ai documenti amministrativi, ex art.10 del predetto TUEL, ovvero ex art.22 e ss. della Legge 241/1990 per coloro che abbiano un interesse tutelato.

In sostanza al consigliere comunale viene riconosciuto un diritto dai confini più ampi, definito dalla giurisprudenza del Consiglio di Stato quale **"incondizionato diritto di accesso"** a tutti gli atti che possano essere d'utilità all'espletamento delle loro funzioni.

Tale diritto di accesso non può essere compresso neppure per esigenze di tutela di riservatezza dei terzi con riferimento ai dati sensibili, eventualmente contenuti nei documenti oggetto di istanza, in quanto il consigliere stesso è tenuto al segreto nei casi specificamente determinati dalla legge.

Nel caso di specie quindi è **stata ritenuta ammissibile** la richiesta del consigliere degli elenchi relativi ai percettori di contributi erogati dal comune per l'emergenza COVID-19.

1 […] I consiglieri comunali e provinciali hanno diritto di ottenere dagli uffici, rispettivamente, del comune e della provincia, nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato. Essi sono tenuti al segreto nei casi specificamente determinati dalla legge.

ORDINI DI SERVIZIO POLIZIA LOCALE: i limiti dell'accesso civico

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI: no all'accesso civico generalizzato ai dati e alle informazioni personali contenute negli ordini di servizio

Non si possono esporre gli affari interni della Polizia Locale ad una normale richiesta di accesso civico[2], in particolare se si tratta di tutelare i dati degli operatori.

Lo ha evidenziato l'Autorità Garante per la protezione dei dati personali con il parere n. 9483596 del 15 ottobre 2020 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9483596), indirizzato al RPCT di un comune al quale era stata presentata istanza per l'accesso ad una serie di documenti interni del comando di polizia locale ovvero ordini di servizio definitivi, registro delle variazioni agli ordini di servizio, disposizioni scritte e indicazioni.

Il Garante **conferma il diniego** alla possibilità di prendere visione di questo tipo di dati, in quanto anche tentando di anonimizzarli, il rischio di ledere i diritti degli interessati resta rilevante perché i dati di dettaglio che restano evidenziati sono tali da agevolare una ricognizione delle persone coinvolte. Si deve infatti tenere conto della tipologia e della natura dei dati, anche di dettaglio, contenuti negli ordini di servizio, quali ad esempio turno di servizio previsto, lavoro svolto, attività da svolgere nel giorno seguente, prestazioni effettive, dati su eventuali assenze programmate o su assenze dal servizio comunicate a seguito di malattie o infortuni, 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, determinando possibili ripercussioni negative sul piano personale, professionale, sociale e relazionale, sia all'interno che all'esterno dell'ambiente lavorativo.

2 **Art. 5. Accesso civico a dati e documenti**
1. L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione.
2. 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, 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, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis.

DATI PATRIMONIALI DEI DIRIGENTI PUBBLICI: pubblicazione a "perimetro ristretto"

TAR LAZIO: non devono essere pubblicati online i dati patrimoniali dei dirigenti che non concorrono alla formazione dell'indirizzo politico, ma svolgono funzioni operative di gestione

Nella recente sentenza 12288/2020 (https://www.progettoomnia.it/download/295002) del 20 novembre , ha annullato la deliberazione 586/2019 dell'ANAC (https://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Atti/Delibere/2019/Del.586.2019.pdf), che aveva "offerto" una lettura riduttiva della sentenza n. 20/2019 della Corte Costituzionale (https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2019&numero=20), ritenendo che «le affermazioni fatte dalla Corte sono impostate secondo una definizione molto ampia di incarico dirigenziale riferita ai soggetti responsabili ad ogni livello del buon andamento della Pubblica Amministrazione».

Si tratta, di fatto, degli obblighi di pubblicazione previsti dall'art.14[3] comma 1 lettera f) del d.lgs 33/2013. Secondo l'ANAC, quella pronuncia avrebbe riguardato direttamente tutti i dirigenti pubblici indipendentemente dalla tipologia di amministrazione presso cui prestano servizio, mentre per i giudici amministrativi laziali il novero dei dirigenti pubblici tenuti alla pubblicazione anche dei dati patrimoniali non può allargarsi a dismisura.

Il caso di specie si riferisce effettivamente al caso di una ASL, dove spesso il numero dei dirigenti è superiore, ma il principio espresso può valere anche in generale creando un precedente.

3 **Art. 14. Obblighi di pubblicazione concernenti i titolari di incarichi politici, di amministrazione, di direzione o di governo e i titolari di incarichi dirigenziali**
1. Con riferimento ai titolari di incarichi politici, anche se non di carattere elettivo, di livello statale regionale e locale, lo Stato, le regioni e gli enti locali pubblicano con riferimento a tutti i propri componenti, i seguenti documenti ed informazioni:
a) l'atto di nomina o di proclamazione, con l'indicazione della durata dell'incarico o del mandato elettivo;
b) il curriculum;
c) i compensi di qualsiasi natura connessi all'assunzione della carica; viaggi di servizio e missioni pagati con fondi pubblici;
d) i dati relativi all'assunzione di altre cariche, presso enti pubblici o privati, ed i relativi compensi a qualsiasi titolo corrisposti;
e) gli altri eventuali incarichi con oneri a carico della finanza pubblica e l'indicazione dei compensi spettanti;
f) le dichiarazioni di cui all'art. 2, della L. 441/1982, nonché le attestazioni e dichiarazioni di cui agli artt. 3 e 4 della medesima legge, come modificata dal presente decreto, limitatamente al soggetto, al coniuge non separato e ai parenti entro il secondo grado, ove gli stessi vi consentano. Viene in ogni caso data evidenza al mancato consenso. Alle informazioni di cui alla presente lettera concernenti soggetti diversi dal titolare dell'organo di indirizzo politico non si applicano le disposizioni di cui all'art. 7.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI: sì al diritto all'oblio (cancellazione) per chi è risultato estraneo a vicende giudiziarie

Una persona ha diritto a veder deindicizzati[4] dai motori di ricerca gli articoli che riportano vicende giudiziarie risalenti nel tempo alle quali è poi risultata estranea. Il principio è stato affermato dall'Autorità Garante per la privacy che ha **dichiarato fondati** i reclami presentati da due persone ed ha ordinato a Google di rimuovere gli url[5] agli articoli reperibili facendo una ricerca online con i loro nominativi.

Nel primo caso, il nominativo compariva in alcuni articoli di stampa che riferivano di un collegamento tra la società, nella quale la persona prestava la propria attività, e un'altra azienda direttamente coinvolta in un'inchiesta giudiziaria. Nel secondo caso, il nominativo era riportato in articoli riguardanti una vicenda giudiziaria in cui erano coinvolte altre persone.

In entrambi gli episodi i reclamanti, che non erano **mai stati sottoposti** a provvedimenti giudiziari (come confermato dai certificati penali), si erano rivolti al Garante lamentando il pregiudizio personale e professionale derivante dalla permanenza in rete degli articoli e chiedendo la rimozione degli url.

Respingendo le tesi di Google che aveva ritenuto non vi fossero i presupposti per l'esercizio del diritto all'oblio, l'Autorità ha affermato invece che la perdurante reperibilità in rete degli articoli associati ai nominativi dei reclamanti crea un impatto sproporzionato sui loro diritti, non bilanciato da un interesse pubblico a conoscere notizie che non hanno avuto alcun seguito giudiziario a loro carico. Il Garante ha quindi **ordinato a Google la rimozione** degli url ed ha disposto l'annotazione nel registro interno dell'Autorità, previsto dal GDPR, della misura adottate nei confronti del motore di ricerca.

4 Il **deindicizzare** significa non rimuovere la pubblicazione (magari è un archivio giornalistico e può ivi restare anche contro la volontà dell'interessato) ma significa impedire che il contenuto venga trovato tramite motori di ricerca esterni, non tramite quello interno del servizio stesso.

5 La locuzione **Uniform Resource Locator** (in acronimo **URL**), nella terminologia delle telecomunicazioni e dell'informatica, è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete di computer, come ad esempio un documento, un'immagine, un video, tipicamente presente su un host server e resa accessibile a un client.

TRASFERIMENTO DATI ALL'ESTERO: nuove clausole contrattuali standard dalla Commissione UE

Un contratto tipo per l'outsourcing: lo ha confezionato la Commissione Europea in applicazione del GDPR. Lo schema di atto interessa tutti i casi in cui un'impresa o una Pubblica Amministrazione si serve di un fornitore esterno per servizi che comportano un trattamento di dati per conto del committente (ad esempio l'affidamento di servizi amministrativi e contabili, servizi di gestione dei servizi informatici, dalla gestione di contatti con la clientela, servizi riguardanti la videosorveglianza, la cura dei siti internet, e così via).

In tutti i casi in cui il fornitore esterno tratta dati per conto del committente, il GDPR obbliga alla sottoscrizione di un **contratto/atto**. **N.B.:** Non si tratta di un adempimento da sottovalutare, perché **in mancanza scatta una sanzione amministrativa** (fino a 10 milioni o, se superiore, per le imprese fino al 2% del fatturato totale mondiale annuo).

Inoltre l'articolo 28 GDPR al paragrafo 9 **impone la forma scritta**, al paragrafo 8 stabilisce che ogni Autorità Garante di ogni stato europeo può stendere **clausole contrattuali tipo**, e, infine, al paragrafo 7 statuisce che le clausole contrattuali tipo possono essere elaborate dalla Commissione UE.

A questo proposito la commissione UE il 19 novembre 2020 ha licenziato le sue clausole standard (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries), che oltre all'articolato propongono un allegato. Ed è proprio l'allegato la sede in cui le parti devono descrivere in dettaglio le caratteristiche del trattamento dei dati e le misure di sicurezza. L'articolato in alcune disposizioni è una riproposizione parafrasata dell'articolo 28 citato.

Va aggiunto che l'articolato è limitato agli aspetti di "privacy" e lascia agli interessati la regolamentazione degli aspetti relativi a compensi e responsabilità. Proprio in punto responsabilità, la regola generale del GDPR è la responsabilità solidale di committente e responsabile esterno di fronte all'interessato.

Quanto all'ambito di applicazione del contratto relativo alla responsabilità del trattamento va ricordato che **si applica anche ai rapporti con le Pubbliche Amministrazioni**, che devono ricordarsi di inserirne uno schema nei documenti delle gare di appalto.

QUESTURA NON RETTIFICA I DATI: il Garante sanziona il Ministero dell'interno

Una questura comunica in modo errato a vari uffici il contenuto di un provvedimento di ammonimento rivolto ad una donna. Ma lo corregge, nonostante la richiesta di rettifica avanzata dall'interessata, solo dopo l'apertura di un formale procedimento da parte del Garante per la protezione dei dati personali, e la stessa Autorità commina al Ministero dell'interno, in quanto Titolare del trattamento, **una sanzione di 50 mila euro.**

La questura, pur sapendo della inesattezza dei dati comunicati, almeno dal giugno 2019, ossia dalla data di richiesta della rettifica della reclamante, non aveva provveduto, considerando sufficiente che fossero corrette le informazioni inserite nel CED del Dipartimento della Pubblica Sicurezza.

Di diverso avviso il Garante, al quale la donna si era rivolta. L'Autorità ha affermato infatti che la presenza dei dati corretti nel CED **non esimeva** la Questura dall'obbligo di rettificare i dati erronei trasmessi ad altri soggetti, obbligo la cui violazione ha determinato una lunga permanenza di dati personali inesatti nei loro archivi. Solo nel luglio 2020, ossia ad oltre un anno dalla richiesta di rettifica e solo dopo la comunicazione dell'avvio del procedimento da parte dell'Autorità, la questura ha inviato a tutti i destinatari della prima comunicazione una nota di rettifica dei dati.

L'Autorità ha precisato che la consapevolezza da parte della questura di avere comunicato ad una pluralità di uffici dati inesatti e la decisione di non procedere subito alla loro rettifica, configura un trattamento illegittimo per violazione del diritto alla tempestiva rettifica dei dati personali errati senza giustificato motivo. Inoltre la condotta omissiva ha leso i diritti della reclamante all'esattezza dei propri dati personali ed alla loro immediata correzione in caso di inesattezza.

L'Autorità, tenuto anche conto della collaborazione poi fornita dalla questura nel corso del procedimento, ha quindi applicato la sanzione minima, pari a 50mila euro, nei confronti del Ministero quale Titolare del trattamento, ordinando alla stessa amministrazione di valutare l'opportunità di **promuovere adeguate iniziative formative nei confronti del personale**, anche periferico, della Polizia di Stato, per assicurare il rispetto dei diritti degli interessati e l'immediata rettifica dei dati inesatti.

WI-FI PUBBLICO GRATUITO: il Garante per la protezione dei dati personali chiede all'AGID più tutele per gli utenti

Misure di sicurezza per evitare accessi alle reti interne della PA, divieto di tracciamenti non necessari degli utenti, conservazione "a tempo" dei dati, maggiore trasparenza. Sono alcune delle importanti garanzie richieste dal Garante per la protezione dei dati personali nel parere reso all'AGID sullo schema di Linee guida sul Wi-Fi pubblico (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9487928). L'AGID (Agenzia per l'Italia Digitale) dovrà integrare lo schema per renderlo conforme alle disposizioni dell'attuale normativa "privacy".

Le Linee guida offrono indicazioni alle PA che forniscono ai cittadini la connessione wireless ad Internet presso gli uffici e altri luoghi pubblici, in particolare nei settori scolastico, sanitario e turistico. L'offerta di tale servizio comporta tuttavia il trattamento, da parte delle amministrazioni, dei dati degli utenti che ne usufruiscono, caratterizzato da diversi profili di rischio.

Per questo motivo l'Autorità ha ritenuto che le Linee guida devono essere integrate al fine di richiamare le Pubbliche Amministrazioni a garantire una corretta applicazione della normativa mediante l'adozione di misure tecniche ed organizzative adeguate al rischio e configurando il servizio in modo da assicurare la protezione dei dati trattati fin dalla progettazione e per impostazione predefinita (Privacy by Design e by Default).

Lo schema sottoposto al Garante raccomanda, in particolare, alle PA di identificare gli utenti, per poter rintracciare eventuali comportamenti malevoli. Su questo punto, l'Autorità ha precisato che le amministrazioni non sono autorizzate a conservare dati di traffico telematico e ha chiesto all'AGID di integrare le Linee guida indicando alle amministrazioni modalità alternative per individuare, a posteriori, i responsabili di condotte illecite (ad es. utilizzando i soli dati relativi alla connessione/disconnessione).

L'Autorità ha chiesto inoltre di fornire **indicazioni** alle amministrazioni **sulle tipologie di dati da raccogliere e sui tempi di conservazione**, nel rispetto del principio di minimizzazione. Dovrà essere vietato qualunque trattamento di dati relativi ai dispositivi degli utenti a fini di tracciamento dell'ubicazione o degli spostamenti, consentendo SOLO l'uso di quelli indispensabili per l'accesso al servizio o per individuare, a posteriori, eventuali illeciti.

È possibile, inoltre, che il servizio di Wi-Fi free pubblico venga offerto anche ai turisti, attraverso le strutture alberghiere. Al riguardo, il Garante ha richiesto che lo schema venga integrato precisando che il turista deve poter decidere autonomamente se aderire al servizio di Wi-Fi free in interoperabilità o utilizzare la sola connettività alberghiera. L'eventuale interoperabilità non deve automaticamente prevedere la comunicazione alle amministrazioni dei dati dei clienti degli alberghi.

Infine, le Linee guida dovranno ribadire alle PA la necessità di adottare adeguate misure di sicurezza, anche per la gestione delle violazioni di dati personali (artt. 32, 33 e 34 del GDPR), nonché suggerire specifiche cautele nel caso in cui il servizio Wi-Fi free sia utilizzato anche dai dipendenti della Pubblica Amministrazione che lo fornisce.

REDDITO DI CITTADINANZA: Ok del Garante "privacy" all'incrocio dei dati per i controlli dell'INPS

Sono state approvate dal Garante per la protezione dei dati le misure che l'INPS adotterà per acquisire, anche in modo massivo, sulla base di apposite convenzioni da stipularsi con diversi soggetti pubblici, le informazioni necessarie per effettuare i controlli sulla concessione del reddito di cittadinanza (RdC). Il parere favorevole dell'Autorità (https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9487928) è stato reso sullo schema di provvedimento dell'INPS.

I trattamenti di dati che l'INPS dovrà svolgere, infatti, pur essendo finalizzati all'esecuzione di un compito di interesse pubblico, presentano rischi elevati per i diritti e le libertà degli interessati, in quanto prevedono scambi di dati personali (su larga scala e con modalità telematiche), dati relativi alla salute, alla condizione sociale e alla situazione economica e finanziaria, nonché a condanne penali e reati, riferiti principalmente a soggetti vulnerabili, a volte anche minori d'età.

I dati oggetto di scambio tra l'INPS e le diverse amministrazioni (tramite ad esempio Anagrafe tributaria), dovranno quindi essere limitati a quelli strettamente necessari ad effettuare le verifiche previste (ad esempio possesso di beni immobili, intestazione di autoveicoli, ricovero in strutture pubbliche, condanne o misure cautelari personali).

Dovranno essere adottate, inoltre, adeguate misure di sicurezza volte ad assicurare l'integrità e la riservatezza dei dati sia con riferimento ai flussi informativi (ad es., mediante tecniche in grado di assicurare la cifratura delle informazioni e la firma digitale) sia con riferimento ai trattamenti effettuati dalle amministrazioni che detengono i dati (che potranno trattare i dati dei beneficiari solo per il tempo necessario ad effettuare le verifiche, rendendoli incomprensibili ai soggetti non autorizzati e disponendo la loro immediata cancellazione una volta fornite le informazioni all'INPS).

Il Garante, infine, nel prendere atto di quanto dichiarato dall'INPS (ossia il rispetto dei criteri anche per le verifiche sulla permanenza dei requisiti), si riserva di verificare la conformità al GDPR di tali successivi controlli nell'ambito della Valutazione di Impatto (DPIA) più generale che verrà predisposta dall'INPS.

Le misure di garanzia approvate, consentendo l'incrocio dei dati, confermano il presidio dell'Autorità teso a **favorire l'erogazione del reddito di cittadinanza solo a coloro che ne hanno diritto** e per i quali risulti dimostrato il reale stato di necessità.

TELEMARKETING AGGRESSIVO. Dal Garante sanzione a Vodafone per oltre 12 milioni di euro

Il Garante per la protezione dati personali ha ordinato a Vodafone il pagamento di una sanzione di **oltre 12 milioni e 250 mila euro** per aver trattato in modo illecito i dati personali di milioni di utenti a fini di telemarketing. Oltre al pagamento della multa, la società dovrà adottare una serie di misure dettate dall'Autorità per conformarsi alla normativa nazionale ed europea sulla tutela dei dati.

Il provvedimento conclude una complessa istruttoria avviata dal Garante a seguito di centinaia di segnalazioni e reclami di utenti che lamentavano continui contatti telefonici indesiderati, effettuati da Vodafone e dalla sua rete di vendita, per promuovere i servizi di telefonia e internet offerti dall' azienda.

Nel corso dell'istruttoria è emerso, in particolare, un allarmante utilizzo di numerazioni fittizie o comunque non censite nel **Registro degli Operatori di Comunicazione (ROC)**[6].

Un fenomeno, avvertito dalla stessa Vodafone, che sembra ricondursi in massima parte ad un "sottobosco" di call center abusivi, che effettuano attività di telemarketing in totale spregio delle disposizioni in materia di protezione dei dati personali. Ulteriori profili di violazione sono stati rilevati nella gestione delle liste dei nominativi da contattare acquisite da fornitori esterni.

Sono risultate inadeguate anche le misure di sicurezza dei sistemi di gestione della clientela, profilo sul quale l'Autorità aveva già ricevuto numerosi reclami e segnalazioni da parte di clienti che erano stati contattati da sedicenti operatori Vodafone, i quali chiedevano l'invio di documenti di identità mediante Whatsapp, probabilmente con finalità fraudolente.

Il Garante, infine, ha vietato a Vodafone ogni ulteriore trattamento di dati con finalità promozionali o commerciali svolto mediante l'acquisizione di liste anagrafiche da soggetti terzi, senza che questi ultimi abbiano acquisito un consenso specifico, libero e informato dagli utenti.

6 Il **Registro degli Operatori di Comunicazione**, comunemente definito **ROC**, è uno specifico elenco al quale debbono obbligatoriamente iscriversi i soggetti destinatari di concessioni o autorizzazioni in materia di comunicazione (imprese concessionarie di pubblicità da trasmettere mediante impianti radiofonici o televisivi o su giornali quotidiani/periodici, imprese di produzione e distribuzione dei programmi radiofonici e televisivi, imprese editrici di giornali quotidiani, di periodici o riviste e le agenzie di stampa nazionali, le imprese fornitrici di servizi telematici e di telecomunicazioni, compresa l'editoria digitale). La sua tenuta e regolamentazione è affidata all'Autorità per le Garanzie nelle Comunicazioni.