COMUNICAZIONI DELLA CONFEDERAZIONE AGLI ENTI ASSOCIATI

36/2011

AGLI ENTI ASSOCIATI

INFORMAZIONI AMMINISTRATIVE ED APPROFONDIMENTI

INDICE

Limiti assunzionali articolo 14, comma 9 del dl n. 78/2010 – Il limite del 20% vale per ogni tipologia contrattuale – Corte dei Conti Sezioni riunite delib. n. 46/2011

L'articolo 14, comma 9 del dl n. 78/2010 prevede il divieto (per gli enti nei quali l'incidenza delle spese di assunzione è pari o superiore al 40% delle spese correnti) di procedere ad assunzioni di personale a qualsiasi titolo e con qualsivoglia tipologia contrattuale, a decorrere dall'01/01/2011, mentre gli altri enti possono procedere ad assunzioni di personale nel limite del 20% della spesa corrispondente alle cessazioni dell'anno precedente.

Sulla questione del 20% le sezioni regionali della Corte di Conti si sono espresse i modo non univoco in particolare per quanto riguarda la possibilità di assunzione con tipologie di contratto a tempo indeterminato, o di altre tipologie.
Sulla questione si è espressa la Corte dei conti a Sezioni riunite con la deliberazione n. 46 del 29 agosto 2011 affermando che
"Relativamente agli enti locali sottoposti al patto di stabilità interno, l'art. 14, comma 9, seconda parte, del DL 31 maggio 2010 n. 78, convertito nella legge 30 luglio 2010 n. 122, nella parte in cui stabilisce il vincolo di spesa alle assunzioni di personale, deve essere riferito alle assunzioni di personale a qualsiasi titolo e con qualsivoglia tipologia contrattuale. Ciò ferme restando le eccezioni espressamente stabilite per legge, gli interventi caratterizzati da ipotesi di somma urgenza e lo svolgimento di servizi infungibili ed essenziali".

Ministero dell'Interno – Contributo IVA Trasporto Pubblico Locale - Erogato acconto del 70% per l'anno 2011

Il Ministero dell'Interno rende noto che sulla base del certificato trasmesso entro il termine perentorio del 28 febbraio 2011, con D.M. n. 35200 dell'11 agosto 2011 è stato erogato il contributo IVA Trasporto Pubblico Locale pari al 70 per cento degli oneri che gli enti hanno previsto di sostenere per l'anno 2011.

La predetta percentuale è stata applicata sulle somme certificate dagli enti dopo aver preliminarmente detratte le quote dell'imposta spettanti all'Unione Europea e quelle attribuite alle Regioni a statuto speciale, alle province autonome di Trento e Bolzano ed alle regioni a statuto ordinario in base alla vigente normativa.

La presentazione del modello "B" oltre il termine del 28 febbraio 2011 ha comportato per alcuni enti la mancata corresponsione del contributo ma non pregiudica la possibilità, per gli enti stessi, di trasmettere entro il 30 aprile 2012 il modello "B1" indispensabile per l'assegnazione del relativo trasferimento erariale.

Si segnala, inoltre, che con successivo D.M. n. 35632 del 18 agosto 2011 si è provveduto al saldo definitivo del contributo dovuto per l'anno 2009 (modello "B1" presentato entro il 30 aprile 2010).

A seguito di quanto previsto dal decreto legislativo del 14 marzo 2011 n. 23 "Disposizioni in materia di federalismo fiscale municipale" è stata prevista la devoluzione di entrate con corrispondente soppressione dei trasferimenti erariali, pertanto il contributo IVA trasporto pubblico locale è stato inserito tra i contributi fiscalizzati dal decreto del Ministro dell'Interno di concerto con il Ministro dell'Economia e delle Finanze del 21 giugno 2011.

Di conseguenza il pagamento a titolo contributo IVA trasporto pubblico locale derivante dal preventivo 2011 è stato effettuato ai soli comuni della regione Sardegna, alle province, alle unioni di comuni, ai consorzi e alle comunità montane.

Imposta di Bollo – Ministero dell'Interno – Circolare n. 23 del 06 settembre 2011 relativa al rilascio di certificazioni anagrafiche ai sensi dell'art. 18 del d.lgs. n. 112/1999

Il Ministero dell'Interno ha diffuso la Circolare n. 6 in riferimento al rilascio delle certificazioni anagrafiche ai sensi dell'art.18 del d.lgs. n.112/1999 che secondo il Ministero devono essere rilasciate in carta libera.
Dunque non sono soggette all'imposta di bollo le certificazioni anagrafiche rilasciate sia ad Equitalia che a Poste Italiane Spa nell'espletamento del servizio di notifica delle cartelle esattoriali affidatole da Equitalia.

Autorità di Vigilanza sui Contratti Pubblici – Definizione dei contenuti fondamentali dei Bandi Tipo

Lo scorso 14 maggio è entrato in vigore il decreto legge n. 70. L'art. 4, comma 2, lett. h), del d.l. 13 maggio 2011, n. 70 , convertito in legge dalla legge 12 luglio 2011, n. 106, prevede un'importante novità in tema di redazione dei documenti di gara, introducendo, all'articolo 64 del decreto legislativo 12 aprile 2006, n. 163 (di seguito, Codice), il comma 4-bis, secondo cui «i bandi sono predisposti dalle stazioni appaltanti sulla base di modelli (bandi-tipo) approvati dall'Autorità, previo parere del Ministero delle infrastrutture e dei trasporti e sentite le categorie professionali interessate, con l'indicazione delle cause tassative di esclusione di cui all'articolo 46, comma 1-bis. Le stazioni appaltanti nella delibera a contrarre motivano espressamente in ordine alle deroghe al bando-tipo».

La norma opera un esplicito rinvio alle "cause tassative di esclusione", secondo quanto previsto dal nuovo comma 1-bis dell'art. 46 del Codice - parimenti introdotto dall'art. 4, comma 2, lett. d) del citato d.l. n. 70/2011 – secondo il quale le stazioni appaltanti possono escludere i candidati o i concorrenti «in caso di mancato adempimento alle prescrizioni previste dal presente codice e dal regolamento e da altre disposizioni di legge vigenti, nonché nei casi di incertezza assoluta sul contenuto o sulla provenienza dell'offerta, per difetto di sottoscrizione o di altri elementi essenziali ovvero in caso di non integrità del plico contenente l'offerta o la domanda di partecipazione o altre irregolarità relative alla chiusura dei plichi, tali da far ritenere, secondo le circostanze concrete, che sia stato violato il principio di segretezza delle offere; i bandi e le lettere di invito non possono contenere ulteriori prescrizioni a pena di esclusione. Dette prescrizioni sono comunque nulle».

Sulla base di tali disposizioni, quindi, le cause di esclusione devono derivare dalla violazione di norme vigenti e devono essere tipizzate nei bandi-tipo predisposti dall'Autorità. Si prescrive, inoltre, da un lato, la nullità delle ulteriori disposizioni eventualmente previste a pena di esclusione dalle stazioni appaltanti nella *lex specialis* di gara e, dall'altro, la necessità di motivare esplicitamente eventuali deroghe rispetto al contenuto dei bandi-tipo.

Infine, altre rilevanti modifiche sono state apportate sia all'art. 38 del Codice, sui requisiti di ordine generale per la partecipazione alle gare.

Un'ulteriore modifica è, poi, quella apportata dall'art. 4, comma 2, lettera i-bis) del d.l. n. 70/2011 all'articolo 81 del Codice, che disciplina i criteri per la scelta della migliore offerta. Il nuovo comma 3-bis prevede che l'offerta migliore sia «determinata al netto delle spese relative al costo del personale, valutato sulla base dei minimi salariali definiti dalla contrattazione collettiva nazionale di settore tra le organizzazioni sindacali dei lavoratori e le organizzazioni dei datori di lavoro comparativamente più rappresentative sul piano nazionale, e delle misure di adempimento delle disposizioni in materia di salute e sicurezza nei luoghi di lavoro».

L' AVCP, in attuazione di quanto previsto dai dispositivi delle manovre di finanza pubblica, ha predisposto un documento riassuntivo delle maggiori problematiche interpretative sui temi sopra indicati, allo scopo di effettuare una consultazione delle categorie interessate e delle amministrazioni.

Sul sito dell'Autorità sono disponibili i contenuti del documento di consultazione contenente tutte le novità in materia di redazione dei bandi di gara.

Il documento è reperibile su : www.AVCP.it.

All'esito della consultazione e dopo aver acquisito il parere del Ministero delle Infrastrutture ai sensi dell'articolo 64, comma 4 bis del Codice, saranno individuate le clausole tassative di esclusione per i bandi tipo di lavori, servizi e forniture.

Garante della Privacy – Indicazioni per il corretto e consapevole trattamento dei dati personali con riferimento all'impiego di nuovi strumenti di comunicazione e all'erogazione di servizi informatici che comportano l'esternalizzazione di dati, documenti e procedure (cloud computing)

Il Garante della Privacy ha pubblicato una serie di riflessioni e indicazioni per il corretto e consapevole trattamento dei dati personali con riferimento all'impiego di nuovi strumenti di comunicazione, come gli smartphone e i tablet, e all'erogazione di servizi informatici che comportano l'esternalizzazione di dati, documenti e procedure.

Le indicazioni del Garante si propongono di offrire un primo insieme di indicazioni utili a tutti gli utenti di dimensioni contenute e di limitate risorse economiche (singoli, piccole o medie imprese, amministrazioni locali quali i piccoli comuni, ecc.) destinatari della crescente offerta di servizi di *cloud computing* (pubbliche o ibride), con l'obiettivo di favorire l'adozione consapevole e responsabile di tale tipologia di servizi. Tali indicazioni si indirizzano anche ai fornitori, che potranno tenerne conto nella predisposizione dei servizi offerti.

Di seguito le indicazioni per l'utilizzo consapevole dei servizi *cloud* (che comportano l'esternalizzazione di dati, documenti e procedure) – il documento integrale è reperibile su www.garanteprivacy.it:

• *Ponderare prioritariamente rischi e benefici dei servizi offerti*

Prima di optare per l'adozione di servizi di *cloud computing*, è opportuno che l'utente verifichi la quantità e la tipologia di dati che intende esternalizzare (es. dati personali identificativi o meno, dati sensibili oppure particolarmente delicati come quelli genetici o biometrici, dati critici per la propria attività come ad esempio progetti riservati). Tale analisi valutativa dovrà evidenziare l'opportunità o

meno di ricorrere a servizi *cloud* (limitandone l'uso ad esempio a determinati tipi di dati), nonché l'impatto sull'utente in termini economici e organizzativi, l'indisponibilità, pur se parziale o per periodi limitati, dei dati esternalizzati o, peggio, la loro perdita o cancellazione.

• Effettuare una verifica in ordine all'affidabilità del fornitore

Accertare l'affidabilità del fornitore prima di migrare sui sistemi virtuali i propri dati più importanti, tenendo in considerazione le proprie esigenze istituzionali o imprenditoriali, la quantità e la tipologia delle informazioni che intendono allocare nella *cloud*, i rischi e le misure di sicurezza.
Valutare le caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità.

• Privilegiare i servizi che favoriscono la portabilità dei dati

E' consigliabile ricorrere a servizi di *cloud computing* privilegiando servizi basati su formati e standard aperti, che facilitino la transizione da un sistema *cloud* ad un altro, anche se gestiti da fornitori diversi. Ciò al fine di scongiurare il rischio che eventuali modifiche unilaterali dei contratti di servizio da parte di uno qualunque degli operatori che intervengono nella catena di fornitura si traducano in condizioni peggiorative vincolanti o, comunque, per facilitare eventuali successivi passaggi da un fornitore all'altro.

• Assicurarsi la disponibilità dei dati in caso di necessità

Si raccomanda di mantenere una copia di quei dati (anche se non personali) dalla cui perdita o indisponibilità potrebbero conseguire danni economici, per l'immagine o in generale relativi alla missione e alle finalità perseguite dall'utente. Il titolare del trattamento dei dati dovrà comunque provvedere al salvataggio (*backup*) dei dati allocati nella *cloud*, ad esempio creandone una copia locale (eventualmente sotto forma di archivio compresso), allo scopo di gestire gli eventuali rischi insiti nell'acquisizione di servizi .

• Selezionare i dati da inserire nella cloud

Alcune informazioni che si intende inserire sui sistemi del fornitore di servizio, per loro intrinseca natura, quali ad esempio i dati sanitari, genetici, reddituali, biometrici o quelli coperti da segreto industriale, possono esigere particolari misure di sicurezza. In tali casi, poiché dal relativo inserimento nella *cloud* consegue comunque una attenuazione, seppur parziale, della capacità di controllo esercitabile dall'utente, ed una esposizione di tali informazioni a rischi non sempre prevedibili di potenziale perdita o di accesso non consentito, l'utente medesimo dovrebbe valutare con responsabile attenzione se ricorrere al servizio di *cloud computing* oppure mantenere *in house* il trattamento di tali tipi di dati.

• Non perdere di vista i dati

E' sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto anche verificando se i dati rimarranno disponibili nella disponibilità fisica dell'operatore, oppure se questi svolga un ruolo di intermediario, ovvero offra un servizio progettato sulla base delle tecnologie messe a disposizione da un operatore terzo.

• Informarsi su dove risiederanno, concretamente, i dati

Sapere in quale Stato risiedono fisicamente i *server* sui quali vengono allocati i dati, è determinate per stabilire la giurisdizione e la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio. La presenza fisica dei *server* in uno Stato comporterà per l'autorità giudiziaria nazionale, infatti, la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base al singolo ordinamento nazionale. Non è, quindi, indifferente per l'utente sapere se i propri dati si trovino in un *server* in Italia, in Europa o in un imprecisato Paese extraeuropeo.

• Attenzione alle clausole contrattuali

Una corretta e oculata gestione contrattuale può supportare sia l'utente, sia il fornitore nella definizione delle modalità operative e dei parametri di valutazione del servizio, oltre a individuare i parametri di sicurezza necessari per la tipologia di attività gestita. In ogni caso, è importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di *cloud* con riferimento ad obblighi e responsabilità in caso di perdita, smarrimento dei dati custoditi nella nuvola e di conseguenze in caso di decisione di passaggio ad altro fornitore. Costituiscono elementi da privilegiare la previsione di garanzie di qualità chiare, corredate da penali che pongano a carico del fornitore eventuali inadempienze o le conseguenze di determinati eventi (es. accesso non consentito, perdita dei dati, indisponibilità per malfunzionamenti, ecc.). Si suggerisce, inoltre, di verificare eventuali soggetti terzi delegati alla fornitura di servizi intermedi e che concorrono all'erogazione del servizio finale rivolto all'utente, ovvero la preventiva identificazione dei diversi fornitori successivamente coinvolti nel trattamento. Si raccomanda, infine, di accertare quale sia la quantità di traffico dati prevista dal contratto oltre la quale vengono addebitati oneri economici supplementari.

• Verificare le politiche di persistenza dei dati legate alla loro conservazione

In fase di acquisizione del servizio *cloud* è opportuno approfondire le politiche adottate dal fornitore, che si dovrebbero poter evincere dal contratto, relative ai tempi di persistenza dei dati nella nuvola. Da una parte l'utente dovrebbe accertare il termine ultimo, successivo alla scadenza del contratto, oltre il quale il fornitore cancella definitivamente i dati che gli sono stati affidati. Dall'altra, il fornitore dovrà presentare adeguate garanzie, assicurando che i dati non saranno conservati oltre i suddetti termini o comunque al di fuori di quanto esplicitamente stabilito con l'utente stesso. In ogni caso, i dati dovranno essere sempre conservati nel rispetto delle finalità e delle modalità concordate, escludendo duplicazioni e comunicazioni a terzi.

• Esigere e adottare opportune cautele per tutelare la confidenzialità dei dati

Nell'ottica di proteggere la confidenzialità dei propri dati, l'utente dovrebbe valutare anche le misure di sicurezza utilizzate dal fornitore per consentire l'allocazione dei dati nella *cloud*. In generale si raccomanda di privilegiare i fornitori che utilizzano a tal fine tecniche di trasmissione sicure, tramite connessioni cifrate (specie quando i dati trattati sono informazioni personali o comunque dati che devono restare riservati), coadiuvate da meccanismi di identificazione dei soggetti autorizzati all'accesso, la cui complessità sia commisurata alla criticità dei dati stessi. Nella maggior parte dei casi risulta adeguato l'utilizzo di semplici meccanismi di identificazione, basati su *username* e *password*, purché le *password* non siano banali e vengano scelte di lunghezza adeguata. Nell'ipotesi in cui il

trattamento riguardi particolari tipologie di dati - quali quelli sanitari, genetici, reddituali e biometrici o, più in generale, dati la cui riservatezza possa considerarsi "critica" - si raccomanda oltre all'utilizzo di protocolli sicuri nella fase di trasmissione, anche la conservazione in forma cifrata sui sistemi del fornitore di servizio.

• *Formare adeguatamente il personale*

Il personale preposto al trattamento di dati attraverso i servizi di *cloud computing* dovrebbe essere sottoposto a specifici interventi formativi, che evidenzino adeguatamente le modalità più idonee per l'acquisizione e l'inserimento dei dati nella *cloud*, la consultazione e in generale l'utilizzo dei nuovi servizi esternalizzati e delle indicazioni sin qui illustrate, allo scopo di mitigare rischi per la protezione dei dati derivanti non solo da eventuali comportamenti sleali o fraudolenti, ma anche causati da errori materiali, leggerezza o negligenza: circostanze queste che potrebbero dare luogo ad accessi illeciti, perdita di dati o, più in generale, trattamenti non consentiti.

Bergamo, 12 settembre 2011

Confederazione delle Province e
dei Comuni del Nord