MULTIBUSINESS s.r.l.

Circolare del 08 Settembre 2020

INDICE

ENTI LOCALI: sanzionati alcuni Comuni e una Regione per illecita diffusione di dati personali

Gli Enti Locali devono **valutare con particolare attenzione** se, in base alla normativa, possono rendere pubblici i dati personali contenuti in delibere e in altri documenti amministrativi. Lo ha ribadito il Garante in alcuni provvedimenti sanzionatori adottati nei confronti di una Regione, di due Comuni e di un'Unione di Comuni.

Il **primo provvedimento** riguarda una Regione che aveva pubblicato sul proprio sito web un documento riguardante l'esecuzione di una sentenza civile relativa a un debito maturato dall'ente. Alle proteste dei segnalanti, l'amministrazione aveva risposto giustificando la pubblicazione sulla base di alcune disposizioni di natura contabile.

Nel caso specifico, però, il Garante ha ricordato che i dati personali contenuti in quei documenti potevano essere giustamente usati per controlli della magistratura contabile sui debiti fuori bilancio, ma che le norme citate **non ne prevedevano la diffusione**.

Tenendo conto della **collaborazione offerta dall'ente** e dell'impegno per la verifica delle misure tecniche e organizzative adottate dal personale per il rispetto della privacy, il Garante ha comminato alla Regione una **sanzione pecuniaria di 4.000 euro**.

L'Autorità ha accolto anche il reclamo nei confronti di due Enti Locali, un Comune e l'Unione Comunale a cui esso appartiene, che avevano pubblicato sui rispettivi siti web, nella sezione amministrazione trasparente e nell'albo online, atti amministrativi riferibili al reclamante, diffondendo anche dati relativi a condanne penali e a reati.

Nel corso dell'istruttoria, le due amministrazioni hanno sostenuto che la pubblicazione fosse obbligatoria ai sensi della normativa sulla trasparenza e sulla pubblicità legale degli atti e che, in ogni caso, la persona interessata fosse difficilmente identificabile, in quanto negli atti amministrativi oggetto di pubblicazione erano riportati solo il numero di matricola o le iniziali del cognome e del nome. Una delle due amministrazioni, tra l'altro, aveva affermato che la pubblicazione era stata avallata anche dal Responsabile per la Protezione dei Dati (RPD/DPO) dell'ente.

Il Garante ha però rilevato che le normative citate **non consentivano** la diffusione di quei dati personali, tra cui quelli relativi a condanne penali e reati. L'interessato, inoltre, poteva facilmente essere identificato dai colleghi, da conoscenti e da numerosi altri soggetti in ambito locale. Il Comune e l'Unione di Comuni hanno ricevuto **due sanzioni pecuniarie rispettivamente di 4.000 e 6.000 euro**.

L'ultimo provvedimento riguarda, invece, un Comune che aveva inviato per posta elettronica, ad alcune testate locali, un "decreto di citazione" con i dati, riferibili anche a vicende penali e a misure di sicurezza e prevenzione, di cinque persone, tra cui tre testimoni citati a comparire. L'ente locale aveva giustificato la trasmissione del documento ai giornalisti con il fine di tutelare la propria immagine ed esercitare il legittimo diritto di critica nei confronti di alcuni attacchi pubblicati sulla stampa.

Anche in questo caso, però, il Garante ha rilevato che la comunicazione di tali dati non fosse giustificata dalla presunta "esecuzione di un compito connesso all'esercizio di pubblici poteri" o da un'altra base normativa, come quella sulla trasparenza. Al Comune è quindi stata **comminata una sanzione di 2.000 euro**.

Il Garante, nell'approvare i provvedimenti e le relative sanzioni, ha ribadito agli enti locali che **il trattamento di dati personali** effettuati da soggetti pubblici **è lecito solo se necessario per adempiere un obbligo legale** al quale è soggetto il Titolare del trattamento oppure per **l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il Titolare. Ha inoltre aggiunto che la 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 di regolamento.

In ogni caso, l'ente locale è tenuto a rispettare i principi indicati dal Regolamento europeo in materia di protezione dei dati personali ("GDPR"), in particolare, quelli di liceità, correttezza e trasparenza nonché di minimizzazione, in base al quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

BUONO MOBILITÀ: via libera del Garante

Parere favorevole dell'Autorità privacy allo schema di decreto che definisce le modalità e i termini per l'erogazione del c.d. "***buono mobilità***" per l'anno 2020 e la disciplina del "***buono rottamazione***", previsti dal relativo Programma sperimentale allo scopo di ridurre le emissioni inquinanti e in risposta ai cambiamenti climatici. Il buono mobilità è destinato ai maggiorenni residenti nei capoluoghi di Regione, nelle Città metropolitane, nei capoluoghi di Provincia e nei Comuni con popolazione superiore a 50.000 abitanti.

Lo schema di decreto - già sottoposto al Garante in una prima versione nel marzo del 2020 - è stato da ultimo modificato tenendo conto delle osservazioni fornite dalla stessa Autorità nel corso di incontri e contatti con i competenti uffici del ministero.

Le osservazioni dell'Autorità hanno riguardato, in particolare, le modalità di accesso all'applicazione web predisposta dal Ministero, le procedure di presentazione della domanda da parte dei potenziali beneficiari, nonché l'accertamento dei dati di questi ultimi attraverso il Sistema Pubblico di Identità Digitale (SPID).

Con le modifiche apportate, lo schema è risultato nel suo complesso conforme alla disciplina in materia di protezione dei dati. Il Garante ritiene però opportuno un perfezionamento del testo nella parte in cui prevede il ricorso alle dichiarazioni sostitutive, che devono essere rese dai beneficiari al momento della richiesta del bonus, al fine di esplicitare ove possibile le modalità e i soggetti presso i quali il Ministero effettua la verifica della sussistenza dei requisiti dichiarati.

Il "buono mobilità" corrisponderà al 60 per cento della spesa sostenuta per l'acquisto di biciclette, anche a pedalata assistita, e di veicoli elettrici, o per l'utilizzo dei servizi di mobilità condivisa a uso individuale. L'importo non sarà comunque superiore a 500 euro.

Ci sarà inoltre un "buono rottamazione", previsto per i residenti nei Comuni sottoposti alle procedure di infrazione comunitaria per la non ottemperanza agli obblighi previsti dalla direttiva sulla qualità dell'aria (2008/50/CE) ammesso anche a favore dei conviventi.

SPESE SANITARIE: via libera dell'Autorità Garante allo schema di provvedimento sulle detrazioni 2020

Spese sanitarie, i dati dei pagamenti con carta nel tracciato della tessera sanitaria. Il ministero dell'economia ha aggiornato le regole per la comunicazione al sistema tessera sanitaria dei dati legati al pagamento delle spese mediche con metodo tracciato per ottenere le detrazioni nel 2021. Né dà notizia il Garante per la privacy dando il **via libera** allo schema di provvedimento.

I dati messi a disposizione, a partire dal primo gennaio, **sono quelli relativi a spese sanitarie e veterinarie** aggregati per tipologia di spesa, da parte del Sistema TS, nei confronti dell'Agenzia delle entrate. Restano esclusi i dati relativi alle spese sanitarie e veterinarie per le quali risulti effettuato il pagamento con strumenti non tracciabili, che comunque saranno comunicati all'Agenzia con un tracciato a parte.

Inoltre nel provvedimento è specificato che la trasmissione dei dati al Sistema TS viene effettuata anche ai fini della disciplina in materia di fatturazione elettronica e di memorizzazione elettronica e trasmissione telematica dei corrispettivi giornalieri, in relazione alle quali viene altresì disciplinata la messa a disposizione dei medesimi dati nei confronti dell'Agenzia delle entrate, per le sole finalità rispettivamente stabilite.

I dati che il sistema trasmetterà sono:

- la **modalità di pagamento** (se effettuato mediante strumenti che consentono la tracciabilità oppure in contanti);
- il **tipo di documento fiscale** (fattura o corrispettivo);
- **l'aliquota** ovvero la natura della singola operazione ai fini Iva con esclusione delle casistiche di spese sanitarie e veterinarie indicate dal comma 680 dell'art. 1 della l. 160/2019.

All'Agenzia non saranno trasmessi i codici fiscali degli assistiti, ma il sistema tessera sanitaria lo manterrà sia per le spese effettuate in contanti e quindi non con mezzi tracciati, sia nel caso in cui il contribuente si opponga alla messa a disposizione dei dati all'Agenzia delle entrate ai fini della predisposizione della dichiarazione dei redditi precompilata, la trasmissione dei dati relativi alle spese sanitarie al Sistema TS senza l'indicazione del relativo codice fiscale.

GARANTE: insediato il nuovo collegio. Pasquale Stanzione Presidente

Si è riunito in data 29 luglio 2020, nella sua nuova composizione, il Garante per la protezione dei dati personali.

Dopo Stefano Rodotà, Francesco Pizzetti, ed Antonello Soro, è quindi **Pasquale Stanzione** il quarto presidente del Garante per la Privacy (eletto all'unanimità), che guiderà l'Authority di Piazza Venezia nel prossimo settennato.

Docente di diritto privato presso la facoltà di Giurisprudenza dell'Università degli Studi di Salerno, e professore straordinario presso l'Università degli Studi Link Campus University di Roma, nella sua carriera Stanzione è stato anche consigliere della Banca d'Italia e giudice tributario, nonché preside della Facoltà di Giurisprudenza dell'Università di Salerno.

La vice presidente di Stanzione (eletta anch'essa all'unanimità), ***Ginevra Cerrina Feroni***, anch'essa giurista, fino alla sua elezione è stata docente di diritto costituzionale italiano e comparato presso il Dipartimento di Scienze Giuridiche dell'Università di Firenze.

Gli altri due componenti della nuova Autorità sono il dott. Agostino Ghiglia e il dott. Guido Scorza.

L'AUGURIO AL PRESIDENTE USCENTE ANTONELLO SORO

Vorremmo rinnovare il nostro ringraziamento al presidente uscente, Antonello Soro ed al suo Collegio, per l'eccezionale lavoro svolto.

INVALIDAZIONE PRIVACY SHIELD: cosa fare adesso?

Come noto la Corte di giustizia dell'Unione europea (CGUE) si è pronunciata lo scorso 16 luglio (c.d. "Sentenza Schrems II") in merito al regime di t**rasferimento dei dati tra l'Unione europea e gli Stati Uniti** invalidando la decisione di adeguatezza del "Privacy Shield, adottata nel 2016 dalla Commissione Europea in seguito alla decadenza dell'accordo "Safe Harbor".

Nella stessa sentenza la CGUE ha inoltre **ritenuta valida** la decisione 2010/87 relativa alle clausole contrattuali tipo (SCC) per il trasferimento di dati personali a incaricati del trattamento stabiliti in Paesi terzi. Il Comitato Europeo per la Protezione dei Dati (EDPB) ha predisposto delle **FAQ** relative alla sentenza Schrems e ai suoi effetti che si sono rivelate utili per risolvere, almeno in parte, alcuni dubbi.

La normativa statunitense cui fa riferimento la Corte (vale a dire l'articolo 702 della FISA e l'Executive Order (EO) 12333) **si applica a qualsiasi trasferimento verso gli Stati Uniti** per via elettronica che rientra nell'ambito di applicazione della suddetta normativa, indipendentemente dallo strumento utilizzato per il trasferimento.

Nello specifico l'EDPB ha precisato che la possibilità o meno di trasferire dati personali sulla base di SCC dipende dall'esito della valutazione che si dovrà compiere, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto. Le misure supplementari dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle SCC e dalle misure supplementari stesse.

Se si è giunti alla conclusione che, tenuto conto delle circostanze del trasferimento e delle eventuali misure supplementari, **non vi sarebbero adeguate garanzie**, **occorre sospendere o porre fine al trasferimento** di dati personali. Tuttavia, se si intende continuare ciononostante a trasferire i dati, occorre informarne la SA competente.

La valutazione della Corte si applica anche con riguardo alle norme vincolanti d'impresa (BCR), in quanto la normativa statunitense prevarrà anche sull'applicazione di quest'ultimo strumento. Anche in questo caso **la possibilità di trasferire** o meno dati personali sulla base delle BCR **dipenderà dall'esito della valutazione**.

Le misure supplementari unitamente alle BCR, alla luce di **un'analisi caso per caso** delle circostanze del trasferimento, dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle BCR e dalle misure

supplementari stesse. In caso contrario si perverrà alle stesse conclusioni già evidenziate per le SCC.

Il Comitato europeo si è inoltre riservato di valutare le conseguenze della sentenza sugli strumenti di trasferimento diversi dalle SCC e dalle BCR. Difatti, la sentenza chiarisce che il parametro per l'adeguatezza delle garanzie di cui all'art. 46 del GDPR è costituito dalla "equivalenza sostanziale". Inoltre l'EDPB ha specificato che **è ancora possibile trasferire dati** dal SEE agli Stati Uniti sulla base delle deroghe previste dall'articolo 49 del GDPR, **purché siano soddisfatte le condizioni** di cui a tale articolo.

In particolare, è opportuno ricordare che, quando i trasferimenti sono basati sul consenso dell'interessato, esso dovrebbe essere: esplicito, specifico con riguardo al particolare trasferimento o insieme di trasferimenti (il che significa che l'esportatore deve assicurarsi di ottenere un consenso specifico prima che il trasferimento sia messo in atto anche se ciò avviene dopo la raccolta dei dati), e informato.

Per quanto riguarda i trasferimenti necessari all'esecuzione di un contratto tra l'interessato e il Titolare del trattamento, occorre tenere presente che i dati personali possono essere trasferiti solo su base occasionale.

In relazione, poi, ai trasferimenti necessari per **importanti motivi di interesse pubblico** (che devono essere riconosciuti nella legislazione dell'UE o degli Stati membri), il Comitato europeo per la protezione dei dati ricorda che il requisito essenziale per l'applicabilità di tale deroga è la constatazione della sussistenza di importanti motivi di interesse pubblico, e non già la natura del soggetto coinvolto nel trasferimento.

In definitiva, quindi, va riconosciuto che l'EDPB nel proprio documento ha sostanzialmente fornito un'interpretazione della "Sentenza Schrems II" **meno "catastrofica"** rispetto ad altre posizioni, riconoscendo la possibilità di trasferimenti verso gli USA sulla base dei più noti strumenti previsti dal GDPR.

Naturalmente la problematica non è affatto semplice, ma come già evidenziato nel documento dobbiamo attenderci ulteriori suggerimenti del Comitato Europeo.

APP COVID: allarme dei medici europei: a rischio privacy dei cittadini

Allarme generale del Comitato Permanente dei Medici Europei (CPME) a seguito delle dichiarazioni del Governo di Londra sulla possibilità effettiva di violazione della privacy degli utenti dopo il download dell'applicazione per il tracciamento dei contatti (*contact tracing*).

Il 20 luglio scorso, il Dipartimento della salute del Governo britannico ha comunicato, in una lettera all'Open Rights Group, la possibilità concreta di una violazione del Regolamento Generale europeo sulla Protezione dei Dati (GDPR).

Il Comitato dei medici europei, in un documento, ha espresso diverse preoccupazioni relative all'uso di tale app e di altre simili per possibili accessi non autorizzati ai dati sensibili delle persone.

I rischi più seri sono stati individuati nella **violazione dei dati sanitari** e **nella raccolta di non autorizzata di dati relativi agli spostamenti e la posizione** degli individui (location data) per finalità che esulano quelle sanitarie. Ma visto che si tratta di accessi non autorizzati a tali dati, la stessa sicurezza informatica dei device è messa a rischio.

Serve quindi una seria Valutazione dell'Impatto (DPIA) delle app dedicate al Covid-19 in termini di sicurezza informatica, di privacy e di trattamento dei dati dei cittadini.

Una valutazione che però, hanno spiegato dal CPME, deve avvenire prima del lancio delle app, non a posteriori (ad app scaricata in sostanza), mentre sono necessarie anche delle **valutazioni periodiche** da cui trarre sempre informazioni aggiornate su quanto accade ai nostri dati.

Violare il GDPR significa andare incontro a sanzioni fino a 20 milioni di euro, o a multe pari al 4% delle entrate globali.

La multa più grande inflitta in Europa, per il violazione del GDPR, è stata decisa in Francia, contro Google nel 2019, per una cifra di 50 milioni di euro.