

Sim aziendali e controllo dei consumi nel rispetto della privacy

Il Garante per la protezione dei dati personali ha pubblicato la Newsletter n. 437 del 26 gennaio 2018 (provvedimento n. 3 del 11 gennaio 2018), con la quale, tra le altre cose, ha fornito il proprio assenso all'utilizzo, da parte dell'azienda, di un sistema per il controllo dei consumi telefonici aziendali sulle SIM fornite ai lavoratori.

.....

Nel sempre discusso e spinoso tema dei controlli sui dipendenti, Vi informiamo che il Garante per la privacy con il provvedimento n. 3 del 11 gennaio 2018 ha dato il via libera ad un sistema per il controllo dei consumi telefonici aziendali.

L'azienda che effettuerà tali controlli dovrà, però, attenersi a precise misure a tutela della riservatezza dei lavoratori.

In particolare, in base al Codice privacy, l'Autorità ha commisurato i tempi di conservazione dei dati entro un limite di 6 mesi.

Il datore di lavoro dovrà informare adeguatamente i dipendenti e adottare un disciplinare interno per regolamentare le condizioni di uso delle SIM in dotazione ai dipendenti.

È stato, inoltre, disposto che il *file* sul quale saranno memorizzati i dati estratti dal portale del fornitore del servizio di comunicazione elettronica dovrà essere protetto mediante opportune tecniche di cifratura e che nell'ambito delle successive elaborazioni i dati dovranno essere anonimizzati mediante l'utilizzo di tecniche che non consentano la re-identificazione dell'interessato.

In particolare, in conformità alla disciplina in materia di protezione di dati personali, il Garante ha prescritto che le informazioni sul traffico telefonico vengano trattate solo se necessarie, pertinenti e non eccedenti, o comunque se, in base alle condizioni contrattuali applicabili dal provider, comportino dei costi (ipotesi che non ricorre per le chiamate in entrata in roaming senza specifici addebiti e in caso di tariffe flat). Sui numeri delle chiamate in uscita e, nei casi consentiti, di quelle in entrata, sarà operato il mascheramento delle ultime quattro cifre.

L'azienda specializzata che effettuerà l'elaborazione di dati verrà designata quale responsabile del trattamento e dovrà restituire i risultati dell'analisi dei consumi a ciascuna società del gruppo solo per il personale di propria appartenenza.

In presenza di “*consumi anomali*”, la società provvederà a rilevarne le cause e, ove necessario, evidenzierà al proprio interno l’esigenza di contenere i costi aziendali, ma i dati non potranno essere trattati a fini disciplinari.

In ogni caso, poiché il sistema è idoneo a realizzare un potenziale e indiretto controllo a distanza sull’attività dei dipendenti, dovrà comunque essere stipulato specifico un accordo sindacale da parte di ciascuna società nel rispetto della disciplina di settore.

Qui di seguito Vi proponiamo il provvedimento nella sua interezza.

L’istanza della società

La Johnson&Johnson Medical S.p.A. (di seguito, la società) - in proprio e per conto delle altre società del Gruppo Johnsons&Johnson in Italia, cioè Johnson&Johnson S.p.A. e Janssen-Cilag S.p.A. - ha presentato una richiesta di verifica preliminare ai sensi dell’articolo 17 del Codice con riguardo al trattamento di dati personali dei propri dipendenti "cui sia stato assegnato un telefono aziendale". Il trattamento avrebbe la finalità di "controllo delle fatture del provider del servizio telefonico" nonché di "analisi dell’andamento complessivo dei consumi in modo da valutare nel tempo l’adeguatezza del contratto con il provider [...] con l’obiettivo di ridurre i costi aziendali e ottimizzare la qualità del servizio" nonché "rilevare eventuali situazioni anomale di consumi". Il trattamento sarebbe effettuato mediante l’adozione di un sistema che consentirebbe di raccogliere ed elaborare i dati personali dei dipendenti ad opera della società inglese Tangoe Europe Limited, specializzata nel settore, che la società istante si impegna a designare responsabile del trattamento ai sensi dell’articolo 29 del Codice (cfr. p. 2 nota 20.12.2016 e p. 2 nota 19.06.2017).

Stando a quanto dichiarato i dati oggetto di trattamento sarebbero "forniti dal provider per ogni bolletta inviata" e consisterebbero nel: "numero chiamato o chiamante, giorno, ora dell’inizio della telefonata, durata della stessa" (cfr. nota del 20.12.2016). Più nel dettaglio, tra le informazioni raccolte figurerebbero le numerazioni delle utenze chiamate, la durata delle comunicazioni, il tipo di servizio utilizzato, i paesi di provenienza o di destinazione della chiamata, l’orario di inizio della chiamata (cfr. all. 1, nota 19.06.2017).

Il livello di aggregazione delle soglie di consumo considerate sarebbe su base bimestrale (cfr. pag. 1, nota del 19.06.2017). La società ha dichiarato che intende attuare specifiche misure a tutela degli interessati, in particolare l’"anonimizzazione dei numeri del chiamante e del chiamato, mediante mascheramento delle ultime quattro cifre".

1.2. A seguito di una richiesta di chiarimenti formulata dall'Autorità la società ha precisato con nota di riscontro del 19 giugno 2017 che:

a. "i dati ricevuti dal fornitore del servizio di comunicazione elettronica [...] riportano i numeri chiamati già oscurati (le ultime 3 cifre sostituite da asterischi) [...] i numeri chiamanti [...] vengono riportati solo nel caso di telefonate in roaming ed anche in questo caso con i numeri già oscurati (le ultime 3 cifre sostituite da asterischi)";

b. le predette società intestatarie delle utenze aziendali avrebbero "comunicato [al fornitore del servizio di comunicazione elettronica] il nominativo e l'indirizzo e-mail aziendale dei rispettivi dipendenti reali utilizzatori dei telefoni e dei dispositivi mobili nei quali sono inserite le schede sim agli stessi assegnate; al riguardo si precisa che uno stesso dipendente può utilizzare più sim [...] e che il contratto con [il fornitore del servizio di comunicazione elettronica] prevede che il fornitore rilev[i] i consumi per ciascun dipendente";

c. "il sistema [...] prevede lo scarico dei dati di dettaglio resi disponibili dal fornitore [...] sul proprio portale in occasione della emissione della fattura bimestrale e l'invio di tali dati alla società inglese Tangoe Europe Limited, con sede a Londra" (cfr. allegato 1 alla nota cit.);

d. le operazioni di trattamento che la società si riserva di effettuare sono "lo scarico delle informazioni e registrazione di dettaglio rese disponibili dal provider di servizi sul proprio portale e registrazione su foglio Excel memorizzato su una cartella riservata del sistema informativo"; "Criptazione del file ed invio a Tangoe (la chiave di criptazione verrà inviata con un messaggio separato)"; "analisi degli addebiti in fattura e verifica della conformità degli stessi all'effettivo utilizzo dei servizi di comunicazione voce e dati di cui al dettaglio fornito dal provider (attività svolta da Tangoe)" "rilevazione di eventuali situazioni anomale di consumi (attività svolta da Tangoe); "analisi dell'andamento complessivo dei consumi in modo da valutare sistematicamente l'adeguatezza nel tempo del contratto con il provider [...] con l'obiettivo di ridurre i costi aziendali e ottimizzare la qualità del servizio; rilevazione di eventuali situazioni anomale di consumi [...] invio a ciascuna delle società dei risultati delle elaborazioni effettuate da Tangoe in relazione alle utenze assegnate ai rispettivi dipendenti; distruzione dei dati di dettaglio in possesso di Tangoe dopo 12 mesi dalla ricezione";

e. l'arco temporale di conservazione fissato in 12 mesi è stato stabilito "in ragione dell'esigenza di realizzare un'analisi di dettaglio dei consumi e dei conseguenti costi aziendali del servizio di comunicazione elettronica";

f. la società provvederà a rendere la dovuta informativa a i dipendenti interessati "in occasione della prima attivazione del servizio";

g. "l'accesso al portale del fornitore del servizio di comunicazione elettronica è consentito con credenziali di accesso individuali [...] i dati saranno registrati in un foglio Excel a cura dell'incaricato che effettua l'accesso e conservati nei sistemi aziendali [...] la comunicazione alla società Tangoe avverrà previa criptazione del file";

h. la società ha stipulato accordo sindacale [...] analoghi accordi saranno richiesti con le Rsu delle altre due società [...];

i. in presenza di "consumi anomali" - che sono stati individuati nelle ipotesi in cui "i costi complessivi in bolletta relativi al dipendente superano del 50% la media dei costi rilevati per tutti i dipendenti nella medesima bolletta"- verrà segnalato al manager del dipendente;

j. "non sono previsti utilizzi per finalità ulteriori [...né] per finalità disciplinari. In caso di consumi anomali [...] la finalità sarà quella di rilevarne le cause e, se necessario, di segnalare al dipendente l'esigenza di contenere i costi aziendali";

k. "oltre a Tangoe [...] e alla linea manageriale del dipendente, effettueranno il descritto trattamento gli addetti all'unità organizzativa "Servizi aziendali" ed il personale IT addetto al servizio informatico aziendale". L'accesso ai dati sarà consentito ai soli incaricati che saranno dotati di credenziali di accesso personalizzate e i dati saranno trattati nel rispetto della disciplina in materia di misure minime di sicurezza.

RILEVATO

2. Liceità del trattamento di dati personali dei dipendenti mediante il sistema di analisi dei consumi del servizio telefonico.

Alla luce della documentazione in atti, emerge che la società intende utilizzare per le dichiarate finalità di riduzione dei costi aziendali mediante verifiche inerenti alla fatturazione e all'andamento dei consumi, nella prospettiva di valutare l'adeguatezza del contratto con il fornitore dei servizi, un sistema di raccolta ed elaborazione di alcuni dati relativi al traffico telefonico del personale assegnatario di una o più sim aziendali. In particolare il trattamento avrebbe ad oggetto informazioni di dettaglio relative alle chiamate in uscita e, in alcuni casi (telefonate in roaming), anche in entrata, sulla base della periodicità della fatturazione bimestrale (cfr. caratteristiche dei trattamenti descritte al punto 1.2).

Il trattamento che la società intende effettuare riguarda dati personali dei dipendenti trattandosi di informazioni relative al traffico telefonico dagli stessi fruito mediante l'uso di una o più sim aziendali in dotazione (artt. 4, commi 1, lett. b) del Codice). Da ciò consegue l'applicabilità al trattamento in esame della disciplina in materia di protezione dei dati personali, ferme restando le specifiche garanzie previste dal Codice e dalla disciplina di settore in materia di fatturazione del traffico telefonico (cfr. artt. 123, 124 e 132 del Codice; cfr altresì provv.to del Garante 13 marzo 2008 in materia di fatturazione dettagliata, reperibile in www.garanteprivacy.it, doc. web n. **1501106**).

Gli scopi perseguiti con l'installazione del sistema, così come rappresentati dalla società, considerata anche la loro riconducibilità alle legittime esigenze organizzative e di tutela del patrimonio aziendale, risultano in termini generali lecite (art. 11, comma 1, lett. a) e b)).

Tanto, anche alla luce della normativa in materia di controlli a distanza dei dipendenti in osservanza della quale la società, in considerazione del potenziale controllo a distanza (indiretto) sull'attività dei dipendenti suscettibile di essere realizzato attraverso la raccolta dei dati effettuata mediante il menzionato sistema, ha stipulato, in data 13 giugno 2017, specifico accordo con le rappresentanze sindacali nel rispetto della disciplina di settore, fornendo peraltro assicurazioni in merito al non utilizzo delle informazioni "per finalità ulteriori [...né] per finalità disciplinari" (cfr. punto 1.2. lett. j); v. artt. 11, comma 1, lett. a) e 114 del Codice e art. 4, comma 1, l. 20 maggio 1970, n. 300, come modificato dall'art. 23 del d. lg. n. 151/2015).

3. Bilanciamento di interessi

Ciò premesso, anche alla luce delle valutazioni di cui ai successivi paragrafi 4, 5 e 6, relative alla necessità e proporzionalità dei trattamenti in questione e alle misure impartite a tutela degli interessati, il trattamento che la società intende effettuare mediante il descritto sistema risulta in termini generali lecito. Analogamente, la maggior parte delle misure prospettate dalla società e le modalità di configurazione del sistema, risultano proporzionate alle finalità perseguite (art. 1, comma 1, lett. a), d) ed e) del Codice).

Ciò considerato, si ritiene che i descritti trattamenti possano essere effettuati, nei confronti dei dipendenti, per effetto del presente provvedimento che, in applicazione della disciplina sul c.d. "bilanciamento di interessi" (ai sensi dell'articolo 24, comma 1, lett. g) del Codice), individua un legittimo interesse del titolare al trattamento di tale tipologia di dati in relazione alle finalità rappresentate.

4. Principi di necessità e proporzionalità dei trattamenti. Tipologia dei dati e tempi di conservazione.

4.1. In base alla normativa in materia di protezione dei dati personali, per il conseguimento delle finalità legittimamente perseguite potranno formare oggetto di trattamento solo i dati necessari, pertinenti e non eccedenti (artt. 3 e 11, comma 1, lett. d), del Codice).

Pertanto, sotto questo profilo, potranno essere considerati ai fini del trattamento solo quei dati che costituiscano delle specifiche voci di spesa all'interno della fattura comportando un impatto sui costi effettivamente sopportati dalla società, alla luce della tipologia di tariffazione prescelta (tale circostanza ad esempio non ricorre in caso di tariffe c.d. flat).

4.2. Quanto sopra vale anche in relazione al trattamento di informazioni riferite a soggetti terzi nel caso di chiamate in entrata in roaming, (cfr. punto 1.2. lett.a)), quali il numero telefonico "chiamante", i dettagli della chiamata in entrata (giorno, ora dell'inizio della telefonata, durata della stessa) e il Paese di provenienza della chiamata ("source country"; cfr. tabella allegata alla nota 19.06.2017, cit.). Al riguardo, si ritiene che non sia necessario rispetto alla dichiarata finalità di "controllo sulle fatture" emesse dal provider per l'analisi dei consumi "con l'obiettivo di ridurre i costi aziendali e ottimizzare la qualità del servizio", a meno che in base alle condizioni contrattuali applicabili tale tipo di chiamata non comporti specifici costi per la società, documentati in fattura.

4.3. Quanto ai tempi di conservazione dei dati, la disciplina di protezione dei dati personali fa salva la possibilità di conservare i dati personali trattati dal sistema "per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati" (art. 11, comma 1, lett. e), del Codice).

La commisurazione dei tempi effettuata dalla società in dodici mesi non risulta, sotto tale profilo, conforme al predetto principio e a quello di pertinenza e non eccedenza (art. 11, comma 1, lett. d), del Codice).

Tanto, anche in considerazione del fatto che in base alla disciplina di settore, la conservazione dei dati relativi al traffico telefonico strettamente necessari a fini di fatturazione e di documentazione in caso di contestazione, possono essere trattati e conservati dallo stesso fornitore del servizio per un arco temporale non superiore a sei mesi (art. 123, comma 2, del Codice).

Pertanto, al fine di omogeneizzare i tempi di conservazione per finalità di fatturazione alla luce della richiamata disciplina dettata dal Codice in tale ambito, risulta giustificata la conservazione da parte della società dei dati per finalità di "controllo sulle fatture", anche in vista di contenimento dei costi o di eventuali contestazioni, entro un limite temporale non superiore comunque ai sei mesi.

5. Misure ed accorgimenti posti a tutela dei diritti degli interessati.

In ragione delle caratteristiche della soluzione proposta dalla società, è opportuno indicare ulteriori misure aggiuntive rispetto a quelle individuate dalla medesima.

5.1. Nel prendere atto che in presenza di "consumi anomali" la società si limiterà a informare il manager del dipendente affinché questi provveda a invitarlo a contenere i costi (cfr., punto 1.2. lett. i) e j)) e che "non sono previsti utilizzi per finalità [...] disciplinari", si rileva che la società non ha dato conto dell'adozione di una policy aziendale sulle condizioni di utilizzo delle sim da parte dei dipendenti cui sono assegnate.

Per quanto non emerga che in presenza di fruizione del traffico telefonico per finalità personali i relativi costi vengano addebitati al dipendente ovvero venga a questi richiesto un corrispettivo, tuttavia – tenuto conto che la società intende raccogliere ed elaborare i dati di traffico dei dipendenti – si ritiene necessario adottare un disciplinare interno per regolare sia le condizioni di utilizzo delle sim, sia gli altri profili relativi ai trattamenti che si intendono effettuare, da pubblicizzare adeguatamente e da sottoporre ad aggiornamento periodico.

Sotto tale profilo, ove la società – diversamente da quanto emerge dalla documentazione in atti – intenda addebitare specifici costi ai dipendenti in relazione al traffico telefonico fruito per esigenze personali, si rammenta che in ogni caso i numeri di telefono riguardanti tali chiamate non dovranno essere raccolti e che dovrà essere assicurato agli interessati un separato sistema di addebito e tariffazione.

5.2. Il file sul quale, a cura dell'incaricato della società, sono memorizzati i dati estratti dal portale del fornitore del servizio di comunicazione elettronica deve essere protetto mediante opportune tecniche di cifratura, che si andranno ad aggiungere alle misure di protezione già implementate per i tutti i trattamenti della società stessa.

Infine, i dati di fatturazione utilizzati al fine di effettuare "...l'analisi dell'andamento complessivo dei consumi in modo da valutare sistematicamente l'adeguatezza nel tempo del contratto con il provider, e quindi eventualmente modificarlo, con l'obiettivo di ridurre i costi aziendali e ottimizzare la qualità del servizio..." devono essere anonimizzati, mediante l'utilizzo di tecniche di anonimizzazione che non consentano la re-identificazione dell'interessato.

6. Adempimenti previsti dalla legge.

Resta fermo che la società, prima dell'inizio dei descritti trattamenti - come del resto, per alcuni aspetti, già rilevato nell'istanza - è tenuta in base alla normativa vigente a:

- a) fornire ai dipendenti della società coinvolti dai descritti trattamenti, un'informativa comprensiva di tutti gli elementi contenuti nell'articolo 13 del Codice (tipologia di dati, finalità e modalità del trattamento, compresi i tempi di conservazione), anche in conformità al principio di correttezza in base al quale il titolare è tenuto a rendere chiaramente riconoscibili*

agli interessati i trattamenti che intende effettuare e le relative modalità (art. 11, comma 1, lett. a) e 13 del Codice);

b) adottare le misure di sicurezza previste dagli articoli 31 ss. del Codice al fine di preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati;

c) designare Tangoe Europe Limited responsabile del trattamento ai sensi dell'articolo 29 del Codice, come peraltro è stato dichiarato nell'istanza di verifica preliminare, a cura di ogni singolo titolare del trattamento, che dovrà provvedere a fornire opportune istruzioni affinché i dati dei dipendenti siano trattati e conservati separatamente in relazione a ciascuna società dalla quale dipendono; alle singole società dovranno essere resi i risultati dell'analisi dei consumi con riferimento al solo personale di propria appartenenza;

d) predisporre misure al fine di garantire agli interessati l'esercizio dei diritti previsti dagli articoli 7 e seguenti del Codice.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell'articolo 17 del Codice, a conclusione della verifica preliminare, ammette il trattamento di dati personali da parte di Johnson&Johnson Medical S.p.A, Johnson&Johnson S.p.A. e Janssen-Cilag S.p.A., ciascuna con riguardo ai propri dipendenti, mediante il sistema di raccolta, analisi ed elaborazione dei dati come illustrato in motivazione, e prescrive, nell'eventualità in cui venisse avviato il trattamento, che le menzionate società, quali misure necessarie:

a) trattino i dati – anche con riferimento alle chiamate in entrata in roaming - solo se in base alle condizioni contrattuali applicabili tale tipo di chiamata comporti specifici costi per la società, nei termini di cui in motivazione (cfr. punto 4.1.);

b) commisurino i tempi di conservazione dei dati trattati entro un limite temporale non superiore comunque ai sei mesi (punto 4.2.);

c) adottino un disciplinare interno per regolare sia le condizioni di utilizzo delle sim, sia gli altri profili relativi ai trattamenti che si intendono effettuare, nei termini di cui in motivazione (punto 5.1.);

d) adottino le tecniche di cifratura e di anonimizzazione indicate al punto 5.2.

Ai sensi degli articoli 152 del Codice e 10 del decreto legislativo n. 150 del 2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.