



Newsletter

NOTIZIARIO SETTIMANALE
ANNO XV
WWW.GARANTEPRIVACY.IT

NEWSLETTER N. 395 del 3 novembre 2014

- [Lavoro: uso dei dati di localizzazione solo con precise garanzie](#)
- [Scuola: nessun dato sulla disabilità dei docenti nelle graduatorie on line](#)
- [Furti di identità: via libera al sistema di prevenzione](#)
- [Cambiavalute: sì alle comunicazioni sulle negoziazioni](#)

Lavoro: uso dei dati di localizzazione solo con precise garanzie

Un'icona dovrà essere ben visibile sullo smartphone del dipendente

Due società telefoniche potranno utilizzare i dati di localizzazione geografica, rilevati da una app attiva sugli smartphone in dotazione ai lavoratori, purché adottino adeguate cautele a protezione della loro vita privata. Lo ha stabilito il Garante privacy nell'accogliere le istanze di verifica preliminare [doc. web n. [3505371](#) e [3474069](#)] presentate dalle due società che intendono utilizzare questa tipologia di dati per ottimizzare l'impiego delle risorse presenti sul territorio e migliorare la gestione, il coordinamento e la tempestività degli interventi tecnici.

A tutela della riservatezza dei dipendenti l'Autorità ha prescritto l'adozione di una serie di accorgimenti e stringenti misure di sicurezza. Lo smartphone per le proprie caratteristiche è destinato a "seguire" la persona che lo possiede, senza distinzione tra tempo di lavoro e tempo di non lavoro. Il trattamento dei dati di localizzazione può presentare, quindi, rischi specifici per la libertà (es. di circolazione e di comunicazione), i diritti e la dignità del dipendente. Per questo motivo, le società, che si sono anche impegnate a raggiungere un accordo con le organizzazioni sindacali, dovranno adottare specifiche misure volte a garantire che le informazioni visibili o utilizzabili dalla app siano solo quelle di geolocalizzazione, impedendo l'accesso ad altri dati, quali ad esempio, sms, posta elettronica, traffico telefonico. E dovranno configurare il sistema in modo tale che sullo schermo dello smartphone compaia sempre, ben visibile, un'icona che indichi ai dipendenti che la funzione di localizzazione è attiva.

I dipendenti dovranno essere ben informati sulle caratteristiche dell'applicazione (ad es., sui tempi e le modalità di attivazione) e sui trattamenti di dati effettuati dalle società. Nel dare l'ok il Garante ha ritenuto che il sistema sottoposto alla sua attenzione rispetti nel complesso i principi



stabiliti dal Codice privacy. Il sistema infatti è conforme al principio di liceità perché consente di ottimizzare la gestione degli interventi tecnici, incrementando la velocità di risposta alle richieste dei clienti, soprattutto in caso di emergenze o calamità naturali.

La localizzazione geografica, inoltre, rafforza le condizioni di sicurezza dei dipendenti permettendo l'invio mirato di soccorsi in caso di difficoltà. Il sistema risulta poi conforme anche ai principi di necessità, pertinenza e non eccedenza. La rilevazione dei dati di geolocalizzazione prospettata dalle società, infatti, non sarebbe continuativa, ma avverrebbe a intervalli stabiliti. E' previsto che l'ultima rilevazione cancelli quella precedente. Come stabilito dal Codice privacy, prima di attivare il sistema le società dovranno notificare all'Autorità il trattamento di dati sulla localizzazione.

Scuola: nessun dato sulla disabilità dei docenti nelle graduatorie on line

Vietato diffondere informazioni sulla salute

Stop alla pubblicazione on line di graduatorie scolastiche in cui sia indicata la disabilità dei docenti. Il Garante privacy ha dichiarato illecito [doc. web n. [3505289](#)] il trattamento di dati effettuato da un Ufficio scolastico regionale e ha vietato l'ulteriore diffusione in Internet di informazioni sulla salute e di altri dati non pertinenti riferiti a decine di insegnanti.

Sul sito web dell'Ufficio, come segnalato da un insegnante, risultavano infatti pubblicate le graduatorie dei docenti e i rispettivi allegati tra i quali gli elenchi dei "riservisti, gruppo 2: disabili art. 1, l. n. 68/99", corredati da una legenda che dava conto dei benefici connessi, come la precedenza nell'assegnazione della sede per le persone con gravi invalidità e i relativi titoli di preferenza per gli insegnanti non vedenti. Le graduatorie, per di più, recavano in chiaro, oltre ai dati identificativi degli interessati, il codice fiscale e il numero di figli a carico, informazioni risultate eccedenti e non pertinenti rispetto alle finalità della pubblicazione. Inoltre, i dati in questione erano immediatamente reperibili in rete tramite l'inserimento delle generalità degli interessati nei più diffusi motori di ricerca.

Oltre al provvedimento di divieto, il Garante ha prescritto all'Ufficio scolastico regionale di conformare per il futuro la pubblicazione di atti e documenti in Internet alle disposizioni del Codice privacy e delle Linee guida in materia di trasparenza e pubblicità, di recente adozione, rispettando in particolare il divieto di diffusione dei dati idonei a rivelare lo stato di salute degli interessati e le indicazioni fornite dal Ministero dell'Istruzione dell'Università e della Ricerca attraverso apposite circolari. L'Autorità si è riservata inoltre di valutare, con separato provvedimento, gli estremi per contestare all'Ufficio scolastico regionale la violazione amministrativa prevista per l'infrazione del Codice.



Furti di identità: via libera al sistema di prevenzione

Parere favorevole su due convenzioni che ne regoleranno il funzionamento

Il Garante privacy ha espresso parere favorevole su due schemi di convenzione che consentiranno il funzionamento del sistema di prevenzione delle frodi nel settore del credito al consumo, con particolare riferimento ai furti di identità. Il sistema, basato su un archivio centrale informatizzato, sarà gestito da Consap Spa su incarico del Ministero dell'economia e delle

finanze (MEF) e consentirà, tra l'altro, di consultare le banche dati di numerosi enti pubblici (Agenzia delle Entrate, Ministero dell'interno, Ministero dei trasporti e delle infrastrutture, INPS, INAIL) per scoraggiare fenomeni di sostituzione di persona, ad esempio con la falsificazione di documenti.

La prima convenzione [doc. web n. [3505427](#)] definisce le regole a cui devono sottostare le società che ricevono una domanda di finanziamento o altri servizi, i cosiddetti aderenti diretti (banche, intermediari finanziari, fornitori di servizi di comunicazione elettronica o di altri servizi, imprese di assicurazione) per poter accedere al sistema. Le società potranno così verificare l'autenticità dei dati contenuti nella documentazione presentata dalla persona richiedente e controllare eventuali informazioni relative a rischi di frode in corso o frodi già perpetrate.

La seconda convenzione [doc. web n. [3487835](#)] regola invece l'attività dei cosiddetti aderenti indiretti - ovvero i gestori di sistemi di informazioni creditizie (SIC) e le imprese che offrono servizi assimilabili - che le banche e gli altri aderenti diretti possono incaricare come loro intermediari per accertare, tramite il sistema, la veridicità della documentazione presentata.

Vista la particolare delicatezza delle informazioni trattate sono state previste, anche su indicazione del Garante, precise misure al fine di impedire eventuali trattamenti illeciti dei dati delle persone che desiderano usufruire del credito al consumo. Le società potranno utilizzare solo i dati pertinenti e non eccedenti, necessari al perseguimento delle specifiche finalità indicate nel regolamento di attuazione del sistema di prevenzione e nelle specifiche convenzioni inerenti il settore commerciale di appartenenza. Tutti i soggetti coinvolti dovranno inoltre proteggere i dati personali con adeguate misure di sicurezza e potranno conservarli solo per il tempo strettamente necessario.



Cambialvalute: sì alle comunicazioni sulle negoziazioni

Via libera [doc. web n. [3487879](#)] del Garante privacy su uno schema di decreto del Ministro dell'economia in base al quale chi esercita professionalmente l'attività di cambialvalute dovrà comunicare mensilmente all'Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi (Oam) l'elenco di tutte le negoziazioni effettuate e i dati identificativi dei clienti.

Lo schema approvato prevede che vengano trasmesse per via telematica tutte le informazioni relative alle negoziazioni: i dati identificativi dei clienti (nome, cognome, luogo e data di nascita, paese di residenza, estremi del documento di identità) e i dettagli delle singole operazioni (luogo e data, importo e tipo di valuta). L'Oam che per legge ha il compito di conservare i dati per dieci anni dovrà anche predisporre idonei sistemi di salvataggio dei dati e di disaster recovery per ripristinare le funzionalità del sistema informatico in caso di incidenti.

Tuttavia, poiché lo schema di decreto stabilisce che i cambialvalute trasmettano i dati avvalendosi di un servizio presente sul portale dell'Oam secondo le modalità stabilite dallo stesso, senza fornire altre indicazioni, l'Autorità ha chiesto di integrare lo schema prevedendo che il provvedimento, con il quale l'Oam dovrà individuare le modalità di trasmissione dei dati, anche sotto l'aspetto tecnico, sia adottato previo parere del Garante.

L'ATTIVITÀ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÙ

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

- Privacy e sicurezza. Soro risponde a Tricarico - [Comunicato del 23 ottobre 2014](#)
- Trasparenza: il Presidente dell'Anac e il Presidente del Garante per la privacy scrivono al Ministro per la semplificazione e la Pubblica Amministrazione - [Lettera del 30 ottobre 2014](#)

NEWSLETTER

del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).

Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n. 121 - 00186 Roma.

Tel: 06.69677.2752 - Fax: 06.69677.3755

Newsletter è consultabile sul sito Internet www.garanteprivacy.it



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

[Vedi anche newsletter del 3 novembre 2014](#)

[doc. web n. 3474069]

Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 2014

Registro dei provvedimenti
n. 401 dell'11 settembre 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

ESAMINATA la richiesta di verifica preliminare presentata da Ericsson Telecomunicazioni s.p.a. ai sensi dell'art. 17 del Codice;

VISTI gli atti d'ufficio;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la prof.ssa Licia Califano;

PREMESSO

1. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone.

1.1. Ericsson Telecomunicazioni s.p.a. (di seguito: la società) ha presentato il 1° aprile 2014 una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, in relazione al trattamento di dati personali connesso all'attivazione di una nuova funzionalità di localizzazione di dispositivi smartphone che verrebbero forniti in dotazione dalla società ai propri dipendenti nell'ambito di un sistema di Work Force Management (WFM) già esistente.

Tali dispositivi, dotati di GPS (Global Positioning System) capace di effettuare la localizzazione geografica "con un'accuratezza di 31 m circa", sarebbero in grado di comunicare al sistema WFM la propria posizione con una periodicità temporale prestabilita pari a 15 minuti. Il dato relativo alla geolocalizzazione così raccolto non sarebbe acquisito in modo permanente dal sistema bensì automaticamente cancellato in modo tale che "sarà disponibile solo l'ultimo dato di localizzazione pervenuto, ovvero la nuova posizione rilevata annulla e sostituisce la precedente" (cfr. comunicazione dell'1.4.2014, par. 1, "Chiarimenti sul funzionamento del sistema di geo-localizzazione"). Secondo quanto dichiarato dalla società, pertanto, tramite l'attivazione di tale funzionalità "non viene mantenuto e non si ha a disposizione il tracciamento del percorso. Il sistema mantiene solo i dati master (ad esempio siti, attrezzature, ecc) mentre i dati transazionali (ad esempio dettaglio dei WO) vengono eliminati dal sistema dopo 16 giorni dalla chiusura. Dopo questo periodo di tempo i dati vengono distrutti" (cfr. comunicazione cit., par. 4, "Storicizzazione delle informazioni").

I dati personali complessivamente trattati dal sistema sarebbero: "cognome, nome, Service Area, Skill tecnico (es. radio, transmission, power, ecc), Home Base (ovvero dove il tecnico prende servizio), Attività svolta, dato dell'ultima localizzazione rilevato tramite funzionalità GPS dell'applicazione" (cfr. comunicazione cit., par. 4, "Trattamento Dati e Principio di base").

Gli scopi che la società intende perseguire (cfr. comunicazione cit., par. 2, "Specifiche delle esigenze che impongono l'introduzione del sistema di geo-localizzazione") attraverso l'attivazione della menzionata funzionalità di localizzazione sono:

a. disporre l'intervento di propri tecnici in modo tale da consentire il rispetto dei termini contrattuali stipulati con i clienti, che risultano "particolarmente stringenti in quanto l'attività di manutenzione condotta [dalla società] deve supportare la continuità del servizio pubblico offerto dal cliente, inclusa la pronta gestione dei ripristini in caso di emergenze non ultime quelle generate da disastri naturali/ambientali";

b. intervenire (più) rapidamente con personale specializzato in caso di calamità naturali;

- c. migliorare il coordinamento operativo dei "circa 330 tecnici dislocati sul territorio", in modo tale da poter "indirizzare prontamente i tecnici in servizio con le idonee competenze più prossimi al sito oggetto dell'intervento richiesto";
- d. incrementare la sicurezza dei tecnici stessi in caso di incidenti o situazioni di difficoltà.

Ciò posto, "nessun utilizzo dei dati potrà avvenire per finalità diverse da quelle dichiarate, come ad esempio per scopi disciplinari".

Precisato pertanto che la funzione di geolocalizzazione "sarà finalizzata alla sola gestione operativa delle attività di manutenzione", secondo quanto dichiarato, non sono conseguentemente previste forme di interazione "con altri sistemi aziendali quali, a mero titolo esemplificativo, quelli deputati al time reporting" (cfr. comunicazione cit., par. 5, "Interazione tra il sistema di geo-localizzazione ed ulteriori sistemi/strumenti elettronici aziendali").

La società ha inoltre dichiarato che fornirà ai tecnici specifiche istruzioni operative in ordine alla attivazione e disattivazione della "applicazione GPS [...] per rendere possibile l'utilizzo alternativo dello «smart phone» durante l'orario di lavoro (con tracking GPS) e fuori orario di lavoro (senza GPS tracking)"; sarà inoltre data indicazione di "mantenere tale funzionalità attiva durante l'orario di lavoro fatti salvi gli usuali casi di interruzione previsti dal [...] rapporto di lavoro, quali ad esempio il proprio turno mensa" (cfr. comunicazione cit., par. 4, "Attivazione e Disattivazione dell'applicazione"). La società ha inoltre dichiarato che provvederà a fornire agli interessati un'apposita informativa relativa alle caratteristiche del trattamento, anche attraverso la predisposizione di uno specifico "protocollo" (cfr. comunicazione cit., par. 7, "Informativa degli interessati").

Per quanto riguarda, infine, il rispetto della disciplina vigente in materia di controlli a distanza dei dipendenti la società si è impegnata "ad adottare le garanzie previste dall'art. 4 comma 2 della L. n. 300 del 1970 e quindi a raggiungere un accordo con le OO.SS. o, in difetto, ad acquisire l'autorizzazione del competente organo del Ministero del Lavoro e delle politiche sociali" (cfr. comunicazione cit., par. 6, "Liceità del trattamento e bilanciamento di interessi").

1.2. A seguito di una richiesta di chiarimenti ed integrazioni formulata dall'Autorità (in data 7.5.2014), la società ha successivamente precisato che:

- a. il trattamento di dati personali relativi alla localizzazione dei dispositivi smartphone avviene mediante accesso dell'utente "all'applicazione «WFM Click Mobile Touch» attraverso un'autenticazione basata su userid e password"; la password deve essere modificata dopo il primo accesso rispettando determinati requisiti minimi di sicurezza (cfr. nota del 20.5.2014, p. 1);
- b. la possibilità tecnica di accedere alla posizione geografica del dispositivo in un momento dato al di fuori dell'intervallo temporale prestabilito (15 minuti) "non sussiste" (cfr. nota cit., p. 5);
- c. i dati c.d. transazionali, "di natura operativa e [che] contengono le informazioni relative agli ordinativi di lavoro [...] sono memorizzati localmente e quindi sono presenti solo sul dispositivo mobile. [...] L'operazione di cancellazione compiuta dall'utente tramite la funzione «clear stored data» determina la rimozione dei suddetti dati dal dispositivo mobile" (cfr. nota cit., p. 5);
- d. posto che "al termine dell'orario di lavoro ovvero in occasione delle consentite interruzioni dell'attività lavorativa (es. pausa pranzo) il dipendente può disattivare manualmente l'applicazione" in ogni caso, anche qualora il dipendente non provvedesse alla disattivazione manuale "l'applicazione si disattiverà automaticamente dopo 120 minuti di inattività" (cfr. nota cit., p. 5);
- e. in caso di furto o smarrimento del dispositivo si prevede "l'immediato blocco dell'utenza mobile attraverso la denuncia alle AA.GG. e la richiesta di blocco all'operatore telefonico" (cfr. nota cit., p. 6);
- f. quanto ai tempi di conservazione "il sistema WFM, relativamente ai dati di localizzazione, mantiene solo la località di partenza del FT e l'ultima posizione conosciuta. Nessuna informazione storica relativa alla localizzazione è mantenuta nel Sistema" (cfr. All. nota cit., punto 2.4 "Conservazione dei dati").

1.3 Con successiva nota del 30.6.2014, rispondendo ad ulteriori richieste dell'Autorità, la società ha infine specificato che:

- a. "le informazioni che saranno scambiate tra il tecnico di campo ed il sistema WFM sono esclusivamente finalizzate all'assegnazione e gestione dei work order, non sono previste alla data interazioni con altre informazioni presenti sul dispositivo mobile (es. dati di traffico telefonico, sms, posta elettronica o altro)"; la società, in proposito, intende impartire ai dipendenti apposite istruzioni relative alla necessaria adozione di "misure organizzative procedurali da osservare per evitare trattamenti di dati non attinenti ai work order quali ad esempio: non riportare in eventuali aree di commento disponibili con gli SMS o email scambiate con il WFM riferimenti alla vita privata dei singoli, disattivare l'applicazione di

geolocalizzazione presente sullo smart-phone al di fuori degli orari di lavoro" (cfr. nota 30.6.2014, p. 2);

b. il sistema consente (così rettificando quanto affermato in precedenti comunicazioni all'Autorità) la visualizzazione in tempo reale del dato di localizzazione benché "solo ed esclusivamente [in relazione] ad esigenze di assegnazione e gestione dei work order ai tecnici di campo, per soddisfare i requisiti dei servizi operati sulle reti dei Clienti operatori di telecomunicazioni" (cfr. nota cit., p. 3).

2. Trattamento di dati personali dei dipendenti attraverso la localizzazione di dispositivi smartphone.

Il trattamento di dati personali che la società ha sottoposto a verifica preliminare è connesso all'attivazione di un'applicazione (Click Schedule) del sistema di gestione della mano d'opera già in uso (WFM), in grado di interagire – attraverso l'applicazione ClickMobile-WAP – con i dispositivi mobili geolocalizzati (smartphone) posti in dotazione ai tecnici che effettuano interventi sul campo.

Tale trattamento, rispetto alle ipotesi prese in considerazione dall'Autorità nel provvedimento di carattere generale n. 370 del 4 ottobre 2011, relativo all'utilizzo di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro [in www.garanteprivacy.it, doc. web n. [1850581](#)], presenta caratteristiche particolari proprio in considerazione dell'utilizzo di un dispositivo smartphone messo a disposizione dei dipendenti allo scopo di procedere alla raccolta dei dati di localizzazione. Tali dispositivi, in considerazione delle normali potenzialità d'uso nonché in ragione dell'utilizzo oramai comune degli stessi, possono essere agevolmente impiegati anche per finalità diverse da quelle lavorative. Tali ulteriori (e comuni) modalità di impiego sono d'altra parte (ragionevolmente) consentite dalla società (cfr. punto 1.1 laddove ci si riferisce all'"utilizzo alternativo dello «smart phone» durante [...] e fuori [l']orario di lavoro"). Inoltre lo smartphone è, per le proprie caratteristiche, destinato inevitabilmente a "seguire" la persona che lo possiede, indipendentemente dalla distinzione tra tempo di lavoro e tempo di non lavoro.

Il descritto trattamento pertanto presenta rischi specifici per la libertà (es. di circolazione e di comunicazione), i diritti (v. artt. 10, D.Lg. 276/2003 e 8, l. n. 300/1970) e la dignità del dipendente e richiede una specifica ed attenta valutazione da parte dell'Autorità.

3. Liceità del trattamento dei dati di localizzazione: bilanciamento di interessi.

3.1 Le finalità del trattamento, così come rappresentate dalla società, risultano lecite. La funzionalità di localizzazione geografica consente infatti di ottimizzare la gestione ed il coordinamento degli interventi effettuati dai tecnici sul campo, incrementandone la tempestività a fronte delle richieste dei clienti, soprattutto in caso di emergenze e/o calamità naturali. La localizzazione consente altresì di rafforzare le condizioni di sicurezza del lavoro effettuato dai tecnici stessi, permettendo l'invio mirato di eventuali soccorsi soprattutto in aree remote o non facilmente raggiungibili e comunque di supportare più rapidamente i lavoratori in caso di difficoltà.

I trattamenti di dati personali, pertanto, sarebbero effettuati nell'ambito del rapporto di lavoro per soddisfare esigenze organizzative e produttive ovvero per la sicurezza del lavoro, coerentemente con quanto stabilito dalla disciplina di settore in materia di controllo a distanza dei dipendenti (cfr. artt. 11, comma 1, lett. a) e 114 del Codice e 4, legge n. 300/1970). In proposito la società ha dichiarato che le informazioni riferibili ai possessori dei dispositivi saranno utilizzate per finalità non riconducibili a quelle di controllo degli stessi, tanto che nessun "utilizzo dei dati potrà avvenire per finalità diverse da quelle dichiarate, come ad esempio per scopi disciplinari" (comunicazione 1.4.2014, par. 2.3). Il menzionato sistema, sempre in base a quanto sostenuto, non potrà interagire con altri sistemi aziendali, compresi quelli volti a valutare il corretto adempimento della prestazione lavorativa.

3.2 Pertanto, considerato anche che la società ha dichiarato che procederà ad attivare le procedure previste dall'art. 4, comma 2, della legge n. 300/1970 visto che la localizzazione di dispositivi associati a dipendenti identificati può comportare il controllo a distanza dell'attività degli stessi, il menzionato trattamento potrà essere lecitamente effettuato anche senza il consenso degli interessati, per effetto del presente provvedimento che, in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g) del Codice), individua un legittimo interesse al trattamento di tale tipologia di dati (diversi da quelli sensibili) in relazione alle finalità rappresentate.

4. Principi di pertinenza e non eccedenza del trattamento.

4.1 Il trattamento dei dati di localizzazione per le finalità sopra indicate appare altresì nel complesso conforme ai principi di necessità nonché di pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. d), del Codice), alla luce delle circostanze rappresentate nell'istanza e in particolare considerato che:

a. non si effettuerebbe (di regola) la rilevazione continuativa di dati relativi alla localizzazione geografica dei tecnici

bensì con periodizzazione temporale pari a 15 minuti;

b. il sistema sarebbe configurato in modo tale da memorizzare solo l'ultima informazione relativa alla localizzazione del dispositivo al termine di una determinata sessione di lavoro, procedendo a cancellare automaticamente la rilevazione precedente.

4.2 Tuttavia, posto che la società ha dichiarato che il sistema è configurato in modo tale da consentire agli utenti autorizzati all'accesso la visualizzazione in tempo reale dei dati di localizzazione, anche al di fuori della periodizzazione stabilita in via ordinaria (cfr. punto 1.3, lett. b.), l'Autorità ritiene di prescrivere, come misura posta a tutela dei diritti degli interessati, che tale eventuale trattamento di dati in tempo reale avvenga solo in presenza di specifiche esigenze (ad es. legate al verificarsi di situazioni di emergenza e/o di pericolo per il dipendente), individuate all'interno di appositi protocolli che individuino anche i soggetti legittimati ad accedere con tale modalità al sistema.

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

5.1. Considerate le menzionate potenzialità dei dispositivi smartphone e segnatamente la possibilità di raccogliere per loro tramite, anche accidentalmente, informazioni relative alla vita privata del dipendente, la società dovrà:

a. adottare specifiche misure idonee a garantire che le informazioni presenti sul dispositivo mobile visibili o utilizzabili dall'applicazione installata siano riferibili esclusivamente a dati di geolocalizzazione nonché ad impedire l'eventuale trattamento di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica o altro);

b. configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva; l'icona dovrà essere sempre chiaramente visibile sullo schermo del dispositivo, anche quando l'applicazione Click Mobile Touch lavora in background.

5.2. In applicazione del principio di correttezza (art. 11, comma 1, lett. a) del Codice) i trattamenti in esame devono essere resi noti agli interessati, i quali devono essere posti nella condizione di conoscere chiaramente finalità e modalità del trattamento. A tal fine la società dovrà fornire ai dipendenti una puntuale informativa, comprensiva di tutti gli elementi contenuti nell'art. 13 del Codice.

5.3 Si ritiene inoltre opportuno che tra le istruzioni da fornire ai dipendenti relativamente all'utilizzo del dispositivo, si raccomandi di effettuare periodicamente la pulizia dei dati memorizzati localmente attraverso l'attivazione della funzione "clear stored data" (cfr. punto 1.2, lett. c.), fatte salve eventuali esigenze di conservazione da parte del lavoratore .

6. Adempimenti ulteriori e misure di sicurezza.

6.1. Resta fermo che:

a. considerato che il dispositivo che si intende installare comporta il trattamento di dati relativi alla localizzazione, la società è tenuta ad effettuare la notificazione ai sensi dell'art. 37, comma 1, lett. a), del Codice;

b. la società dovrà attenersi, in quanto applicabili, alle prescrizioni ed alle raccomandazioni contenute nel provvedimento n. 13 del 1° marzo 2007 "Linee guida per posta elettronica e internet" (doc. web n. 1387522) (es. in caso di trattamenti effettuati in occasione della predisposizione di idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati; a seguito della riconsegna del dispositivo per interventi di manutenzione o a seguito della cessazione del rapporto di lavoro);

c. gli interessati potranno esercitare i diritti di cui agli artt. 7 ss. del Codice in relazione ai dati personali che li riguardano rilevati mediante il dispositivo in esame;

d. dovranno essere adottate le misure di sicurezza previste dagli artt. 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.

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'art. 17 del Codice, preso atto della richiesta di verifica preliminare presentata da Ericsson Telecomunicazioni s.p.a. in relazione ai trattamenti da effettuare mediante l'attivazione di una funzionalità di localizzazione di dispositivi mobili smartphone forniti in dotazione ai propri dipendenti per finalità organizzative, produttive e connesse alla sicurezza del lavoro, ritiene ammissibile il trattamento da effettuarsi nei termini di cui in motivazione, fermo restando che:

a. la società, quali misure necessarie, dovrà:

- i. adottare specifiche misure idonee a garantire che le informazioni presenti sul dispositivo mobile visibili o utilizzabili dall'applicazione installata siano riferibili esclusivamente a dati di geolocalizzazione nonché ad impedire l'eventuale trattamento di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica o altro);
 - ii. configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva; l'icona dovrà essere sempre chiaramente visibile sullo schermo del dispositivo, anche quando l'applicazione Click Mobile Touch lavora in background (punto 5.1, lett. b.);
 - iii. consentire l'eventuale trattamento dei dati in tempo reale solo in presenza di specifiche esigenze (ad es. legate al verificarsi di situazioni di emergenza e/o di pericolo per il dipendente), individuate all'interno di appositi protocolli (punto 4.2);
 - iv. consentire l'accesso ai dati trattati ai soli incaricati della società che, in ragione delle mansioni svolte o degli incarichi affidati, possono prenderne legittimamente conoscenza;
- b. la società, quale misura opportuna, dovrà raccomandare ai dipendenti di effettuare periodicamente la pulizia dei dati memorizzati localmente attraverso l'attivazione della funzione "clear stored data", fatte salve eventuali esigenze di conservazione da parte del lavoratore (punto 5.3);
- c. la società dovrà notificare al Garante il trattamento dei dati relativi alla localizzazione (punto 6.1, lett. b);
- d. ai dipendenti della società, unitamente agli elementi previsti dall'art. 13 del Codice, dovranno essere fornite informazioni chiare e complete sulla natura dei dati trattati e sulle caratteristiche del dispositivo, tenuto conto delle finalità mediante lo stesso perseguite (punto 5.2); i dipendenti dovranno altresì essere compiutamente informati sulle ipotesi in cui è consentita la disattivazione della funzione di localizzazione nel corso dell'orario di lavoro nonché circa le eventuali conseguenze nel caso in cui la disattivazione avvenga con modalità non consentite;
- e. la società dovrà attenersi, in quanto applicabili, alle prescrizioni ed alle raccomandazioni contenute nel provvedimento n. 13 del 1° marzo 2007 "Linee guida per posta elettronica e internet" (doc. web n. [1387522](#)) (es. in caso di trattamenti effettuati in occasione della predisposizione di idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati; a seguito della riconsegna del dispositivo per interventi di manutenzione o a seguito della cessazione del rapporto di lavoro);
- f. gli interessati potranno esercitare i diritti di cui agli artt. 7 ss. del Codice in relazione ai dati personali che li riguardano rilevati mediante il dispositivo in esame;
- g. dovranno essere adottate le misure di sicurezza previste dagli artt. 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.

2. ai sensi dell'art. 24, comma 1, lett. g) del Codice, in applicazione della disciplina sul c.d. bilanciamento di interessi, per effetto del presente provvedimento il trattamento descritto può essere effettuato senza che sia necessario acquisire il consenso degli interessati, individuando in capo ad Ericsson Telecomunicazioni s.p.a., in relazione all'installazione di un sistema di localizzazione degli smartphone dati in dotazione ai dipendenti, un legittimo interesse volto a soddisfare esigenze organizzative, produttive e legate alla sicurezza del lavoro previa attivazione delle procedure previste dall'art. 4, comma 2, della legge n. 300/1970 (punto 3.2).

Ai sensi degli artt. 152 del Codice e 10 del d.lg. n. 150/2011, 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.

Roma, 11 settembre 2014

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE



[Vedi anche newsletter del 3 novembre 2014](#)

[doc. web n. 3505371]

Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Wind Telecomunicazioni s.p.a. - 9 ottobre 2014

Registro dei provvedimenti
n. 448 del 9 ottobre 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della prof.ssa Licia Califano, componente, e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

ESAMINATA la richiesta di verifica preliminare presentata da Wind Telecomunicazioni s.p.a. ai sensi dell'art. 17 del Codice;

VISTI gli atti d'ufficio;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la prof.ssa Licia Califano;

PREMESSO

1. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone.

1.1. Wind Telecomunicazioni s.p.a. (di seguito: la società) ha presentato il 28 maggio 2014 una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, in relazione al trattamento di dati personali connesso all'attivazione "di un'innovativa soluzione di Work Force Management (WFM), che prevede, tra l'altro, l'utilizzo di tecniche di geolocalizzazione del dispositivo mobile in dotazione ai [...] dipendenti con qualifica di tecnico di rete" operanti sul territorio (pari a "circa 900" lavoratori; cfr. Allegato tecnico, comunicazione 28.5.2014, p. 4).

La nuova funzionalità di localizzazione di dispositivi smartphone – che verrebbero forniti in dotazione dalla società ai propri dipendenti nell'ambito di un sistema di Work Force Management (WFM) già esistente – verrebbe attivata attraverso l'installazione di ClickSoftware, prodotto che mediante l'utilizzo di una apposita applicazione (ClickMobile Touch) "installata sul dispositivo mobile del tecnico [...] integrerà tutte le funzionalità di dialogo con la piattaforma WFM" (cfr. Allegato cit., p. 6).

1.2 I dati che sarebbero in concreto trattati dalla società attraverso il menzionato sistema, peraltro solo dopo aver fornito agli interessati "una dettagliata informativa [...] che sarà pubblicata sulla intranet aziendale" (cfr. Allegato cit., p. 7), consistono:

- nell'ID del dispositivo aziendale affidato al tecnico;
- nel numero di telefono aziendale;
- nelle coordinate GPS "del tecnico durante lo svolgimento dell'attività operativa";
- nelle coordinate GPS della "home base del tecnico per la determinazione dell'area di competenza".

1.3 Gli scopi che la società intende perseguire attraverso l'attivazione della menzionata funzionalità di localizzazione (cfr. Allegato cit., p. 8) sono volti a:

- a. "migliorare i livelli di servizio, assicurando una pianificazione ottimizzata del lavoro";
- b. "supportare la gestione delle attività d'emergenza [...] mediante la conoscenza della posizione dei tecnici e l'identificazione del tecnico più qualificato e più vicino al sito per il quale è richiesto l'intervento";

c. "supportare le misure di sicurezza a tutela dei tecnici coinvolti in attività di servizio allocate in aree remote e/o disagiate".

Ciò posto, la società ha dichiarato che i dati relativi alla posizione geografica dei dipendenti non saranno utilizzati per finalità diverse da quelle rappresentate "né potranno essere usati [...] per qualsivoglia fine disciplinare".

1.4 Quanto alle modalità del trattamento dei dati relativi alla localizzazione la società (cfr. Allegato cit., p. 9) ha dichiarato che:

- a. l'invio della posizione geografica del dispositivo al sistema di Work Force Management effettuata attraverso l'applicazione ClickMobile "non è continuativo ma periodico; la frequenza di rilevamento dei dati, infatti, è configurabile a sistema mediante un parametro specifico (ogni x minuti) ed è completamente scollegata dalla frequenza di utilizzo";
- b. il dipendente può "abilitare o disabilitare la APP all'inizio e alla fine del servizio, così come durante il servizio stesso, qualora risulti necessario per esigenze personali, compatibilmente con le procedure aziendali in essere";
- c. "la piattaforma WFM gestisce l'informazione relativa all'ultima posizione inviata dal dispositivo mobile del tecnico, cancellando quella immediatamente precedente e l'ultima rilevazione verrà cancellata nel momento in cui termina la sua giornata lavorativa";
- d. "il sistema non esegue alcuna storicizzazione del dato di geolocalizzazione, impedendo sia una visione continuativa della posizione del singolo tecnico sia un'eventuale ricostruzione dei relativi percorsi".

In relazione al descritto sistema verrebbero adottate misure di sicurezza "sia minime che idonee"; inoltre tutti coloro che effettueranno i connessi trattamenti di dati personali verranno designati quali incaricati del trattamento (cfr. Allegato cit., p. 9).

1.5 Quanto all'osservanza della disciplina di settore posta in materia di controlli a distanza dei dipendenti, la società ha rappresentato che "attualmente sono in corso gli incontri [con] le rappresentanze sindacali aziendali per la revisione dell'accordo sindacale, in ossequio al disposto di cui all'art. 4 della L. 300/70" (cfr. Allegato cit., p. 7).

1.2. A seguito di una richiesta di chiarimenti ed integrazioni formulata dall'Autorità (in data 25.6.2014), la società ha successivamente precisato che:

- a. benché l'intervallo temporale preimpostato dal fornitore del software relativamente all'invio delle coordinate riferite alla posizione geografica sia pari a tre minuti, si ritiene "che un intervallo di 10 minuti possa essere idoneo a garantire l'efficacia del sistema" (cfr. punto a), nota del 15.7.2014);
- b. relativamente alla possibilità (o meno) di accedere alla posizione geografica del dispositivo in un momento dato al di fuori dell'intervallo temporale prestabilito, si è ribadito che "il dato rilevato è esclusivamente quello inviato dall'APP secondo la frequenza impostata sul sistema" (cfr. punto b), nota cit.);
- c. ai dipendenti è consentito disattivare la funzionalità di localizzazione "compatibilmente con le occorrenze previste dal contratto (permessi, malattia, etc.) e dalle normative aziendali (es. pausa pranzo)" (cfr. cfr. punto c), nota cit.);
- d. "il dispositivo è ad uso promiscuo ed è pertanto sempre garantito l'utilizzo dello stesso a titolo personale" (cfr. cfr. punto c), nota cit.);
- e. l'applicazione installata sul dispositivo smartphone "non ha nessuna interazione con le informazioni presenti sul dispositivo. [...] La società Click Software, produttore responsabile della progettazione e dello sviluppo della soluzione in oggetto, comunica che non vi sono estensioni diverse dalle funzionalità per la quale l'APP è progettata"; pertanto "l'applicazione non dispone di interfacce [...] in grado di interagire con dati attinenti alla vita privata del dipendente" (cfr. punto d) ed e), nota cit.);
- f. i dipendenti potranno "agire sul dispositivo non solo al fine di disattivare le funzionalità di geolocalizzazione [...] ma anche al fine di disattivare l'App a conclusione dell'attività lavorativa della giornata. Infatti, per garantire la massima autonomia/riservatezza del tecnico nella gestione dell'applicativo installato sul proprio smartphone è esclusa ogni possibilità di interventi da remoto, ivi inclusa la previsione di automatismi finalizzati a disattivare l'APP al termine dell'orario di lavoro" (cfr. punto f), nota cit.);
- g. in caso di furto o smarrimento del dispositivo "il dipendente dovrà seguire quanto indicato nella procedura aziendale, che prevede [...] la disattivazione della scheda Sim e contestualmente il blocco del telefono" (cfr. punto g), nota cit.).

2. Trattamento di dati personali dei dipendenti attraverso la localizzazione di dispositivi smartphone.

Il trattamento di dati personali che la società ha sottoposto a verifica preliminare è connesso all'attivazione di un'applicazione

(ClickSoftware) del sistema di gestione della mano d'opera già in uso (WFM), in grado di interagire – attraverso l'applicazione ClickMobile Touch – con i dispositivi mobili geolocalizzati (smartphone) posti in dotazione ai tecnici che effettuano interventi sul campo.

Il descritto trattamento, rispetto alle ipotesi prese in considerazione dall'Autorità nel provvedimento di carattere generale n. 370 del 4 ottobre 2011, relativo all'utilizzo di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro [in www.garanteprivacy.it, doc. web n. [1850581](#)], presenta caratteristiche particolari proprio in considerazione dell'utilizzo di un dispositivo smartphone messo a disposizione dei dipendenti allo scopo di procedere alla raccolta dei dati di localizzazione. Tali dispositivi, in considerazione delle normali potenzialità d'uso nonché in ragione dell'utilizzo oramai comune degli stessi, possono essere agevolmente impiegati anche per finalità diverse da quelle lavorative. Queste ulteriori (e comuni) modalità di impiego sono d'altra parte, ragionevolmente, consentite dalla società (cfr. punto 1.2 "è (...) sempre garantito l'utilizzo [del dispositivo] a titolo personale"). Inoltre lo smartphone è, per le proprie caratteristiche, destinato inevitabilmente a "seguire" la persona che lo detiene, indipendentemente dalla distinzione tra tempo di lavoro e tempo di non lavoro.

Il descritto trattamento pertanto presenta rischi specifici per la libertà (es. di circolazione e di comunicazione), i diritti (v. artt. 10, D.Lg. 276/2003 e 8, l. n. 300/1970) e la dignità del dipendente e richiede una specifica ed attenta valutazione da parte dell'Autorità.

3. Liceità del trattamento dei dati di localizzazione: bilanciamento di interessi.

3.1 Le finalità del trattamento, così come rappresentate dalla società, risultano lecite. La funzionalità di localizzazione geografica consente infatti di ottimizzare la gestione ed il coordinamento degli interventi effettuati dai tecnici sul campo, incrementandone la tempestività e migliorando la qualità del servizio, soprattutto in caso di emergenze e/o calamità naturali. La localizzazione consente altresì di rafforzare le condizioni di sicurezza del lavoro effettuato dai tecnici stessi, permettendo l'invio mirato di eventuali soccorsi soprattutto in aree remote o non facilmente raggiungibili e comunque di supportare più rapidamente i lavoratori in caso di difficoltà.

I trattamenti di dati personali, pertanto, sarebbero effettuati nell'ambito del rapporto di lavoro per soddisfare esigenze organizzative e produttive ovvero per la sicurezza del lavoro, coerentemente con quanto stabilito dalla disciplina di settore in materia di controllo a distanza dei dipendenti (cfr. artt. 11, comma 1, lett. a) e 114 del Codice e 4, legge n. 300/1970). In proposito la società ha dichiarato che i dati riferiti alla posizione geografica "non verranno in alcun modo utilizzati [...] per finalità diverse da quella rappresentata né potranno essere usati per qualsivoglia fine disciplinare" (cfr. Allegato tecnico, comunicazione 28.5.2014, p. 8).

3.2 Pertanto, considerato anche che la società ha dichiarato di aver attivato le procedure previste dall'art. 4, comma 2, della legge n. 300/1970 visto che la localizzazione di dispositivi associati a dipendenti identificati può comportare il controllo a distanza dell'attività degli stessi, il menzionato trattamento potrà essere lecitamente effettuato anche senza il consenso degli interessati, per effetto del presente provvedimento che, in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g) del Codice), individua un legittimo interesse al trattamento di tale tipologia di dati (diversi da quelli sensibili) in relazione alle finalità rappresentate.

4. Principi di pertinenza e non eccedenza del trattamento.

4.1 Il trattamento dei dati di localizzazione per le finalità sopra indicate appare altresì nel complesso conforme ai principi di necessità nonché di pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. d), del Codice), alla luce delle circostanze rappresentate nell'istanza e in particolare considerato che:

- a. non si effettuerebbe la rilevazione continuativa di dati relativi alla localizzazione geografica dei tecnici bensì con periodizzazione temporale pari a 10 minuti;
- b. il sistema sarebbe configurato in modo tale da trattare l'informazione relativa all'ultima posizione inviata dallo smartphone cancellando quella immediatamente precedente, mentre "l'ultima rilevazione verrà cancellata nel momento in cui termina la sua giornata lavorativa".

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

5.1. Considerate le menzionate potenzialità dei dispositivi smartphone e segnatamente la possibilità di raccogliere per loro tramite, anche accidentalmente, informazioni relative alla vita privata del dipendente, la società dovrà:

- a. adottare specifiche misure idonee a garantire che le informazioni presenti sul dispositivo mobile visibili o utilizzabili dall'applicazione installata siano riferibili esclusivamente a dati di geolocalizzazione nonché ad impedire l'eventuale trattamento di dati ultranei (es. dati relativi al traffico telefonico, agli sms, alla posta

elettronica o altro);

b. configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva; l'icona dovrà essere sempre chiaramente visibile sullo schermo del dispositivo, anche quando l'applicazione Click Mobile Touch lavora in background.

5.2. In applicazione del principio di correttezza (art. 11, comma 1, lett. a) del Codice) i trattamenti in esame devono essere resi noti agli interessati, i quali devono essere posti nella condizione di conoscere chiaramente finalità e modalità del trattamento. A tal fine la società dovrà fornire ai dipendenti una puntuale informativa, comprensiva di tutti gli elementi contenuti nell'art. 13 del Codice.

6. Adempimenti ulteriori e misure di sicurezza.

6.1. Resta fermo che:

a. considerato che il dispositivo che si intende installare comporta il trattamento di dati relativi alla localizzazione, la società è tenuta ad effettuare la notificazione ai sensi dell'art. 37, comma 1, lett. a), del Codice;

b. la società dovrà attenersi, in quanto applicabili, alle prescrizioni ed alle raccomandazioni contenute nel provvedimento n. 13 del 1° marzo 2007 "Linee guida per posta elettronica e internet" (doc. web n. 1387522) (es. in caso di trattamenti effettuati in occasione della predisposizione di idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati; a seguito della riconsegna del dispositivo per interventi di manutenzione o a seguito della cessazione del rapporto di lavoro);

c. gli interessati potranno esercitare i diritti di cui agli artt. 7 ss. del Codice in relazione ai dati personali che li riguardano rilevati mediante il dispositivo in esame;

d. dovranno essere adottate le misure di sicurezza previste dagli artt. 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.

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'art. 17 del Codice, preso atto della richiesta di verifica preliminare presentata da Wind Telecomunicazioni s.p.a. in relazione ai trattamenti da effettuare mediante l'attivazione di una funzionalità di localizzazione di dispositivi mobili smartphone forniti in dotazione ai propri dipendenti per finalità organizzative, produttive e connesse alla sicurezza del lavoro, ritiene ammissibile il trattamento da effettuarsi nei termini di cui in motivazione, fermo restando che:

a. la società, quali misure necessarie, dovrà:

i. adottare specifiche misure idonee a garantire che le informazioni presenti sul dispositivo mobile visibili o utilizzabili dall'applicazione installata siano riferibili esclusivamente a dati di geolocalizzazione nonché ad impedire l'eventuale trattamento di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica o altro);

ii. configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva; l'icona dovrà essere sempre chiaramente visibile sullo schermo del dispositivo, anche quando l'applicazione Click Mobile Touch lavora in background (punto 5.1, lett. b.);

iii. consentire l'accesso ai dati trattati ai soli incaricati della società che, in ragione delle mansioni svolte o degli incarichi affidati, possono prenderne legittimamente conoscenza;

b. la società dovrà notificare al Garante il trattamento dei dati relativi alla localizzazione (punto 6.1, lett. b);

c. ai dipendenti della società, unitamente agli elementi previsti dall'art. 13 del Codice, dovranno essere fornite informazioni chiare e complete sulla natura dei dati trattati e sulle caratteristiche del dispositivo, tenuto conto delle finalità mediante lo stesso perseguite (punto 5.2); i dipendenti dovranno altresì essere compiutamente informati sulle ipotesi in cui è consentita la disattivazione della funzione di localizzazione nel corso dell'orario di lavoro nonché circa le eventuali conseguenze nel caso in cui la disattivazione avvenga con modalità non consentite;

d. la società dovrà attenersi, in quanto applicabili, alle prescrizioni ed alle raccomandazioni contenute nel provvedimento n. 13 del 1° marzo 2007 "Linee guida per posta elettronica e internet" (doc. web n. 1387522) (es. in caso di trattamenti effettuati in occasione della predisposizione di idonee misure di sicurezza per assicurare la

disponibilità e l'integrità di sistemi informativi e di dati; a seguito della riconsegna del dispositivo per interventi di manutenzione o a seguito della cessazione del rapporto di lavoro);

e. gli interessati potranno esercitare i diritti di cui agli artt. 7 ss. del Codice in relazione ai dati personali che li riguardano rilevati mediante il dispositivo in esame;

f. dovranno essere adottate le misure di sicurezza previste dagli artt. 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.

2. ai sensi dell'art. 24, comma 1, lett. g) del Codice, in applicazione della disciplina sul c.d. bilanciamento di interessi, per effetto del presente provvedimento il trattamento descritto può essere effettuato senza che sia necessario acquisire il consenso degli interessati, individuando in capo a Wind Telecomunicazioni s.p.a., in relazione all'installazione di un sistema di localizzazione degli smartphone dati in dotazione ai dipendenti, un legittimo interesse volto a soddisfare esigenze organizzative, produttive e legate alla sicurezza del lavoro previa attivazione delle procedure previste dall'art. 4, comma 2, della legge n. 300/1970 (punto 3.2).

Ai sensi degli artt. 152 del Codice e 10 del d.lg. n. 150/2011, 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.

Roma, 9 ottobre 2014

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE
Soro