Circolare del 25 Luglio 2020

INDICE

IMMUNI E APP REGIONALI: LE FAQ DEL GARANTE 1

GARANTE PRIVACY: MAXI SANZIONE DA 17 MILIONI DI EURO PER WIND TRE. MULTATA ANCHE ILIAD 2

SANZIONE DA 600MILA EURO A GOOGLE PER VIOLAZIONE DEL DIRITTO ALL'OBLIO 4

AUTORITÀ GARANTE: FATTURA ELETTRONICA, DATI ECCESSIVI 5

LA CORTE DI GIUSTIZIA DELL'UE INVALIDA IL 'PRIVACY SHIELD: STOP A TRASFERIMENTI DI DATI NEGLI USA 6

NUOVI VERTICI DEL GARANTE: ECCO CHI SONO I QUATTRO COMPONENTI CHE GUIDERANNO L'AUTORITÀ PER IL PROSSIMO SETTENNATO 7

DATI PERSONALI DEI BAMBINI AFFISSI SULLA PORTA DELL'AULA: SANZIONATA UNA SCUOLA PER VIOLAZIONE DELLA "PRIVACY" 8

ANTICIPO TFR "STATALI":SICUREZZA E PRIVACY A RISCHIO 9

© Copyright Multibusiness Srl – All Rights reserved 2009-2020 –

IMMUNI E APP REGIONALI: LE FAQ DEL GARANTE

Può una Regione consentire l'accesso solo a condizione che l'interessato installi l'app? La mancata installazione dell'app può comportare conseguenze? Quale è la base giuridica delle altre app, utilizzate per il contrasto al COVID 19?

A questi e ad altri quesiti rispondono le FAQ pubblicate dal Garante per la protezione dei dati personali sulle problematiche connesse all'app di tracciamento, nonché di altre app da parte di soggetti pubblici o strutture sanitarie. Le FAQ, disponibili sul sito dell'Autorità all'indirizzo https://www.garanteprivacy.it/temi/coronavirus/faq#contact-tracing, contengono indicazioni di carattere generale, anche ispirate alle risposte fornite a reclami, segnalazioni, quesiti ricevuti dall'Ufficio in questo periodo di emergenza.

Riguardo alle app regionali, il Garante ha chiarito che le persone **non possono essere obbligate ad installarle** e che la mancata installazione non può comportare alcuna conseguenza pregiudizievole o condizionare l'accesso ad aree o territori.

Con specifico riferimento all'app nazionale di *Contact Tracing* (app "Immuni"), già autorizzata dal Garante, l'Autorità ha ribadito che **la sua installazione è su base volontaria** e che dalla mancata installazione non può derivare alcuna conseguenza pregiudizievole (come, ad esempio, limitazioni nella fruizione di beni o servizi).

Le strutture sanitarie che intendono avvalersi di strumenti di telemedicina (app di telediagnosi, teleconsulto, teleassistenza e telemonitoraggio utilizzate dal personale medico) per effettuare diagnosi o terapie a distanza, non devono richiedere uno specifico consenso al trattamento dei dati personali dell'interessato. Per l'utilizzo di app diverse da quelle di telemedicina (quali, ad esempio, app divulgative o app per la raccolta di informazioni sullo stato di salute della popolazione di un dato territorio), è necessario invece il consenso dell'interessato, il quale deve essere adeguatamente informato sull'uso che verrà fatto dei suoi dati.

L'Autorità ha inoltre sottolineato che le app devono trattare solamente i dati strettamente necessari a perseguire le finalità del trattamento, evitando di raccogliere dati eccedenti e limitandosi a richiedere permessi per l'accesso a funzionalità o informazioni presenti nel dispositivo solo se indispensabili.

Amministrazioni pubbliche, Regioni, strutture sanitarie dovranno infine valutare i rischi che potrebbero derivare dall'eventuale trasferimento di dati a terze parti, soprattutto se stabilite al di fuori dell'UE.

GARANTE PRIVACY: MAXI SANZIONE DA 17 MILIONI DI EURO PER WIND TRE. MULTATA ANCHE ILIAD

Il Garante ha sanzionato Wind Tre Spa per circa 17 milioni di euro per "numerosi trattamenti illeciti di dati, legati prevalentemente ad attività promozionali", mentre un altro gestore telefonico, Iliad, "che è stato trovato carente sotto altri profili, in particolare in merito alle modalità di accesso dei propri dipendenti ai dati di traffico", è stato sanzionato per 800.000 euro.

> "Continua l'attività di controllo del Garante per la protezione dei dati personali nei confronti degli operatori telefonici anche a seguito delle centinaia di segnalazioni e reclami che settimanalmente pervengono all'Autorità per lamentare casi di *'marketing selvaggio*' - spiega il Garante in una nota.

Nell'ambito di tali attività di controllo, nella riunione del 9 luglio scorso, l'Autorità ha sanzionato Wind Tre Spa per circa 17 milioni di euro per numerosi trattamenti illeciti di dati, legati prevalentemente ad attività promozionali.

"Il nuovo provvedimento è stato adottato all'esito di una complessa attività istruttoria ed ispettiva. Gli utenti lamentavano la ricezione di contatti promozionali indesiderati, effettuati senza consenso tramite sms, e-mail, fax, telefonate e chiamate automatizzate. In numerosi casi, inoltre i segnalanti dichiaravano di non esser stati messi in grado di poter esercitare il proprio diritto di revoca del consenso o di opposizione al trattamento dei loro dati per finalità di marketing. In altri casi veniva lamentata la pubblicazione di dati personali negli elenchi telefonici pubblici nonostante l'opposizione degli interessati.

Dall'istruttoria è inoltre emerso che **le app MyWind e My3** erano impostate in maniera tale da obbligare l'utente a fornire, ad ogni nuovo accesso, una serie di consensi per diverse finalità di trattamento (marketing, profilazione, comunicazione a terzi, arricchimento e geolocalizzazione), salvo poi consentire di revocarli trascorse 24 ore".

Al di là di queste lacune "di sistema", gli accertamenti hanno messo in luce diversi gravi illeciti nella filiera dei partner commerciali di Wind Tre, anche con **impropria attivazione di contratti**. Per queste violazioni, uno dei partner del gestore telefonico - che aveva sub affidato (peraltro senza alcun atto giuridico) intere fasi dei trattamenti a call-center che raccoglievano i dati illecitamente, **è stato multato per 200mila euro** dal Garante e si è visto imporre il divieto di utilizzare i dati raccolti e trattati da agenti

presenti sul territorio nazionale (denominati “procacciatori”) in totale spregio delle norme in materia di protezione dati. Le argomentazioni portate a propria difesa da Wind Tre e la serie di misure correttive implementate dalla società, anche riguardo alla centralizzazione delle campagne promozionali, non sono state ritenute adeguate dal Garante. Oltre a sanzionare la società telefonica per 16.729.600,00 euro, l’Autorità **ha vietato a Wind il trattamento dei dati acquisiti senza consenso** e le ha ordinato di adottare misure tecniche e organizzative per un effettivo controllo della filiera dei partner, nonché procedure per rispettare la volontà degli utenti di non essere disturbati.

"Nel corso della stessa riunione del 9 luglio, il Garante ha preso in esame anche le risultanze degli accertamenti disposti nei confronti di un altro gestore telefonico, Iliad, che è stato trovato carente sotto altri profili, in particolare in merito alle modalità di accesso dei propri dipendenti ai dati di traffico e che per tali ragioni, è stato **sanzionato per 800.000,00 euro**".

ILIAD VALUTA IL RICORSO:

> "Prendiamo atto con molto stupore della decisione del Garante Privacy poiché abbiamo sempre operato nel massimo rispetto dei nostri utenti e dei loro dati personali. Abbiamo avuto modo di provare al Garante stesso che i nostri sistemi sono sicuri e sono stati predisposti per garantire la maggiore tutela possibile secondo il nuovo approccio e le prescrizioni del GDPR".

E' quanto scrive Iliad in risposta alla multa comminata dal Garante sulla quale l'operatore telefonico "sta analizzando il contenuto della decisione nel dettaglio per valutare se procedere con un ricorso.

> "Ci teniamo a precisare che non è stata accertata alcuna violazione dati né dei diritti degli utenti e che, a differenza degli altri operatori, Iliad non effettua attività di teleselling né marketing aggressivo", conclude la nota.

SANZIONE DA 600MILA EURO A GOOGLE PER VIOLAZIONE DEL DIRITTO ALL'OBLIO (CANCELLAZIONE)

In Belgio l'Autorità per la protezione dei dati ha inflitto una **sanzione da 600.000 euro a Google** per mancato rispetto del "diritto all'oblio". Google aveva respinto la richiesta di un cittadino belga, che ha un ruolo di rilievo pubblico, il quale aveva chiesto di rimuovere i risultati di ricerca che lo riguardavano e ritenuti da lui obsoleti e dannosi dai risultati del motore di ricerca.

Gli articoli e notizie che comparivano nei risultati collegati al nome dell'interessato, si riferivano a denunce infondate di molestie. Nella fattispecie, Google aveva sostenuto che il reclamo era infondato perché era stato proposto contro "Google Belgio", mentre il Titolare del trattamento non era la consociata belga di Google, ma Google LLC, che ha sede in California, negli Stati Uniti.

Ma l'autorità non ha accettato questa tesi. A suo avviso, le attività di "Google Belgio" e Google LLC sono indissolubilmente collegate e la controllata belga può quindi essere ritenuta responsabile. Ciò è fondamentale per garantire una protezione efficace e completa del GDPR in quanto non è facile per un'autorità nazionale in Europa controllata e sanzionare efficacemente una società con sede negli Stati Uniti.

Anche se il Garante belga ha ritenuto Google "negligente" nel decidere di non rimuovere i collegamenti procedendo con la sanzione, la Camera delle controversie ha invece seguito l'argomentazione di Google secondo cui il suo ufficio principale in Europa ("Google Irlanda") non è responsabile della rimozione dai risultati della ricerca.

A seguito del procedimento sanzionatorio, un portavoce di Google ha affermato:

> "Non credevamo che questo caso soddisfacesse i criteri della Corte di Giustizia UE per l'eliminazione delle notizie giornalistiche pubblicate nei risultati di ricerca, ma ritenevamo fosse nell'interesse del pubblico che queste notizie rimanessero ricercabili".

Su quella che è di fatto la multa più alta mai imposta dal Garante privacy del Belgio, Google sostiene fermamente di essersi adoperato strenuamente per "trovare un equilibrio ragionevole tra i diritti di accesso alle informazioni e la privacy delle persone", e per questo ha reso noto di avere intenzione di presentare ricorso in tribunale.

AUTORITÀ GARANTE: FATTURA ELETTRONICA, DATI ECCESSIVI

L'Autorità Garante è categorica sullo schema di provvedimento dell'Agenzia delle entrate che detta le regole tecniche per l'emissione e ricezione delle fatture elettroniche. Si tratta della disciplina *ex art. 14 del Decreto Legge n. 124 del 2019*, già oggetto di rilievi critici della stessa Autorità, ritenendo sproporzionata la memorizzazione di dati non fiscalmente rilevanti e inerenti la descrizione delle prestazioni fornite.

[…] l'articolo consente di memorizzare i file delle fatture elettroniche fino al 31 dicembre dell'ottavo anno successivo a quello di presentazione della dichiarazione di riferimento o fino alla definizione di eventuali giudizi, per l'utilizzo da parte della GdF e dell'Agenzia anche per le attività di analisi del rischio e di controllo fiscale.

Dunque ancora una volta, *con il parere n. 133 del 9 luglio 2020*, l'Authority **BOCCIA** la protezione dei dati dell'E-fattura: "… si ritiene che lo schema di provvedimento disciplini un trattamento di dati in violazione degli artt. 5, 6, 9, 10, 24 e 25 del GDPR), riguardante, senza distinzione alcuna tra tipologie di informazioni o categorie di interessati e dati di dettaglio, **anche ulteriori** rispetto a quelli necessari a fini fiscali […]".

L'Autorità mette Sotto osservazione i dati delle E-fatture, anche molto di dettaglio, volti ad individuare i beni e i servizi ceduti, con la descrizione delle prestazioni, i rapporti fra cedente e cessionario e altri soggetti, riferiti anche a sconti applicati, oltre a dati obbligatori imposti. Attenzione è posta per la presenza, all'interno dei file delle fatture di ulteriori dati, utili alla gestione del ciclo degli operatori, ma non rilevanti a fini fiscali.

Lo schema in esame prevede, senza effettuare alcuna distinzione tra tipologie di dati o categorie di interessati, la memorizzazione e l'utilizzo dei file delle fatture elettroniche che contengono i dati inerenti la natura, qualità e quantità dei beni e servizi oggetto dell'operazione, estendendo così l'oggetto della memorizzazione e l'ambito di utilizzazione dei dati presenti nella fattura. NON VENGONO ESCLUSE neppure alcune tipologie di dati (quali quelli non rilevanti a fini fiscali), suscettibili di comprendere anche dati appartenenti a categorie particolari o l'eventuale sottoposizione dell'interessato a procedimenti penali, come per le fatture relative a prestazioni in ambito forense, né i codici fiscali dei consumatori.

Il Garante **si riserva di intervenire**, con successivo parere, sui prospettati trattamenti effettuati a fini di analisi del rischio.

LA CORTE DI GIUSTIZIA DELL'UE INVALIDA IL 'PRIVACY SHIELD: STOP A TRASFERIMENTI DI DATI PERSONALI NEGLI USA

Con la sentenza nella causa C-311/18 del 16 luglio 2020, la Corte di Giustizia dell'Unione europea HA INVALIDATO il "***Privacy Shield***", ovvero l'accordo largamente diffuso con cui grandi organizzazioni e multinazionali potevano fino ad ora legittimare il trasferimento di dati personali tra Europa e Stati Uniti.

Secondo i giudici della Corte di Giustizia dell'Unione europea, il Privacy Shield non fornisce ai cittadini europei sufficienti garanzie contro le leggi statunitensi in materia di sorveglianza e sicurezza della privacy, e perciò ai sensi del GDPR il trasferimento di dati dall'UE verso un Paese terzo può avvenire, in linea di principio, "SOLO SE TALE PAESE TERZO GARANTISCE UN ADEGUATO LIVELLO DI PROTEZIONE".

Se l'annullamento del Privacy Shield rappresenta una vittoria per gli attivisti della protezione dei dati personali, che da tempo accusavano gli Stati Uniti per le pratiche invasive e di sorveglianza inammissibili sui cittadini europei, la decisione dei giudici adesso creerà notevoli problemi alle multinazionali americane e europee che fanno *Business* proprio sul trasferimento e l'utilizzo di dati personali.

Società come Facebook, Apple, Google, ed Amazon, dovranno quindi ripensare le loro strategie industriali per adeguarsi alla decisione della Corte dell'Unione Europea.

NUOVI VERTICI DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI: ECCO CHI SONO I QUATTRO COMPONENTI CHE GUIDERANNO L'AUTORITÀ PER IL PROSSIMO SETTENNATO

Dopo oltre un anno di attesa dalla scadenza dell'attuale Collegio dell'Autorità Garante, rimasto finora in carica in regime di "prorogatio", martedì 14 luglio 2020 i due rami del Parlamento hanno eletto i quattro nuovi componenti che guideranno i vertici del Garante per la protezione dei dati personali nel prossimo settennato.

I due membri nominati dal Senato sono Agostino Ghiglia (con 123 voti), giornalista ed ex deputato, e il giurista Pasquale Stanzione (121 voti), professore di diritto privato presso la facoltà di Giurisprudenza dell'Università degli Studi di Salerno.

La Camera dei deputati ha invece eletto la professoressa Ginevra Cerrina Feroni (209 voti), docente di diritto costituzionale Italiano e comparato presso la facoltà di scienze giuridiche dell'Università di Firenze, e Guido Scorza (237 voti), avvocato cassazionista specializzato in diritto delle nuove tecnologie, privacy e proprietà intellettuale, noto esperto della materia, che da anni offre i suoi contributi ed i suoi interventi a molteplici eventi organizzati per gli addetti ai lavori del settore della protezione dei dati personali.

CHI RICOPRIRÀ LA CARICA DI PRESIDENTE?

L'art. 153 del Codice della Privacy richiede una "comprovata esperienza nel settore della protezione dei dati personali, con particolare riferimento alle discipline giuridiche o dell'informatica".

Di contro l'art. 3 del Regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante, i componenti del nuovo collegio eleggono nel loro ambito il presidente con voto a maggioranza, "ma in caso di parità diventa presidente il componente più anziano di età", e in questo caso sarà Pasquale Stanzione, classe 1945, quello che potrebbe assumere la presidenza per i prossimi sette anni dell'Autorità.

DATI PERSONALI DEI BAMBINI AFFISSI SULLA PORTA DELL'AULA: SANZIONATA UNA SCUOLA PER VIOLAZIONE DELLA "PRIVACY"

Duemila euro di multa per aver diffuso i dati personali degli alunni affiggendoli sulla porta della scuola. Nei giorni scorsi l'Istituto Comprensivo di Uggiano è stato sanzionato dal Garante per la protezione dei dati personali. Al centro della questione c'è quanto avvenuto nel mese di marzo dello scorso anno nella scuola dell'Infanzia di Otranto, dipendente dal Comprensivo di Uggiano; sulla porta dell'edificio erano stati affissi alcuni elenchi che riportavano i nomi degli alunni, le loro date di nascita, gli indirizzi di residenza e i numeri di telefono. In cima agli elenchi, poi, c'era la dicitura, scritta a matita, «manca copia vaccini».

A segnalare l'accaduto al Garante era stata la presidente del comitato «Colibrì» di Nardò. L'istituto scolastico, dal canto suo, si è giustificato sostenendo che gli elenchi erano stati affissi per mero errore, che le liste erano state subito rimosse, che la dicitura «manca copia vaccini» non si riferiva in alcun modo ai nomi indicati e che sarebbero stati attuati provvedimenti disciplinari nei confronti di chi aveva affisso gli elenchi.

Al termine dell'istruttoria, il presidente dell'Autorità Antonello Soro si è pronunciato sulla vicenda, multando la scuola. Il Garante ha sottolineato che la scuola «ha effettuato un trattamento non conforme alla disciplina rilevante in materia di protezione dei dati personali, consistente nella divulgazione di dati e informazioni personali relativi a minori in assenza di un idoneo presupposto».

Ha escluso, comunque, che la diffusione abbia riguardato i dati sulla salute dei minori, poiché tutti gli alunni nell'elenco erano in regola con gli obblighi vaccinali.

Per il Garante, «le memorie difensive prodotte dall'Istituto non hanno prodotto elementi tali da determinare l'archiviazione del procedimento». Da qui la multa, pari a 2.000 euro (ridotta a 1.000 se pagata entro un mese), con la sanzione accessoria della pubblicazione del provvedimento sul sito del Garante.

ANTICIPO TFR "STATALI": SICUREZZA E PRIVACY A RISCHIO

Privacy non garantita dallo schema di accordo quadro sull'anticipo del TFR ai dipendenti pubblici: ma si può rimediare. Questo il parere dell'Autorità Garante (*provvedimento del 9 luglio 2020 n. 131*); parere molto atteso, poichè indispensabile nell'iter di un intervento previsto nel Decreto del 2019 (sul reddito di cittadinanza).

L'intervento è motivato dal fatto che questa operazione implica lo scambio di dati tra più soggetti (pubblici e privati), e può trattarsi di dati molto delicati, che bisogna proteggere. L'anticipo, infatti, verrà erogato dalle banche che scambiano informazioni con l'INPS o altri soggetti erogatori del TFS/TFR. Da qui la necessità di analizzare tutti i profili relativi alla riservatezza degli interessati.

RIPERCORRIAMO I TERMINI DELLA QUESTIONE.

L'articolo 23 del Decreto Legge 4/2019 (reddito di cittadinanza e pensioni) ha previsto la possibilità per i dipendenti pubblici di avere un anticipo dell'indennità di fine servizio/trattamento di fine rapporto: è un finanziamento (massimo 45 mila euro), erogato dalle banche e garantito dalle spettanze di fine rapporto. Le condizioni di questo finanziamento devono essere stabilite con un accordo quadro tra MEF, ministero del lavoro, ministero della P.A. e Associazione Bancaria Italiana, sentito l'INPS.

Con DPCM n. 51 del 22 aprile 2020 è stato adottato il regolamento attuativo del citato articolo 23. L'articolo 15 del DPCM ha dato alcuni dettagli dell'accordo quadro, precisando che nell'iter di stesura dello stesso si dovesse chiedere il parere del Garante della privacy, anche in relazione alla disciplina dei flussi informativi. Ora è stata predisposta una bozza dell'accordo quadro, che è arrivata sulla scrivania del Garante.

E il Garante ha dato il proprio parere, sottolineando le precauzioni da adottare. Sono prescrizioni di carattere tecnico. Si tratta delle misure che possano garantire la sicurezza delle comunicazioni di posta elettronica certificata tra banche e soggetti erogatori. Tali misure non sono specificate nella bozza di accordo; a tal proposito il Garante sottolinea che le stesse devono essere presenti, ma possono essere inserite o nella redazione finale dell'accordo o in successivi documenti tecnici attuativi. Il Garante dà anche indicazioni dei contenuti di queste misure, come modalità di autorizzazione dei soggetti che hanno accesso ai dati e registrazione delle operazioni effettuate, anche con tecniche di cifratura. Lo stesso Garante infine ha chiesto di predisporre informative chiare agli interessati, soprattutto in relazione ai casi in cui la domanda di anticipazione non venga accettata.