Comunicazione e Terziario Avanzato

LUGLIO 2021

Servizi di recapito certificato qualificato: al via i test

Previsti dal Regolamento eIDAS, i Servizi di Recapito Certificato Qualificato, erano ancora rimasti inattuati, ma con le piattaforme che saranno sviluppate dai vari provider, sostituiranno a breve la PEC.
AgID sta mettendo in campo tutte le risorse necessarie per preparare la migrazione verso tali nuovi servizi e insieme ai gestori PEC ha condotto i test utili alla realizzazione di tali servizi di recapito a norma Eidas.
Il 30 maggio 2021 sono iniziati i Plugtests ETSI (European Telecommunications Standards Institute) relativi alla sperimentazione dei servizi REM di recapito certificato e sono terminati il 16 luglio scorso.
Protagonisti di questi Plugtests sono stati i Gestori PEC italiani e AGID che, sulla base del documento pubblicato a fine maggio 2021 dal Gruppo di Lavoro coordinato da AgID, hanno sottoposto i loro

formati alla piattaforma resa disponibile da ETSI, dando un contributo rilevante per la definizione e il consolidamento di quelli che saranno gli standard ETSI a regime.

Si sono accreditati alla piattaforma ETSI 40 soggetti appartenenti ai seguenti Paesi:

- per l'Europa: Austria, Bulgaria, Francia, Germania, Grecia, Ungheria, Italia, Moldavia, Polonia, Regno Unito, Portogallo, Slovacchia, Slovenia, Spagna, Svezia;
- per il resto del mondo: Colombia, Costa Rica, Giappone, Messico.

Riferimenti: art. 44 Regolamento (UE) 910/2014; comunicato AGID del 16/07/2021

Intelligenza Artificiale: predisposta bozza di regolamento UE

Il 21 aprile scorso la Commissione Europea ha presentato la propria proposta di Regolamento per un approccio europeo. Finalità è quella di introdurre una disciplina uniforme e condivisa tra gli Stati membri nell'ottica di garantire i diritti e le libertà fondamentali dei cittadini europei.
l'Intelligenza Artificiale è definita come l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività.

L'IA permette ai sistemi di capire il proprio ambiente, mettersi in relazione per percepire e risolvere problemi e agire verso un obiettivo specifico, con capacità di adattare il proprio comportamento analizzando gli effetti delle azioni precedenti e lavorando in autonomia.
La proposta valuta i rischi connessi all'IA, quali l'abuso, difficoltà nell'individuazione delle responsabilità, perpetuare distorsioni strutturali, minacciare la privacy: non deve essere usata per risolvere complesse questioni sociali; in un incidente in cui è coinvolta un'auto a guida autonoma, è una sfida importante stabilire chi è responsabile per i danni cagionati; la modalità di progettazione e i dati che vengono immessi influenzano i risultati prodotti dall'AI e se alcuni aspetti non venissero programmati o programmati per riflettere distorsioni, come falsare decisioni in merito a un'assunzione o la concessione di prestiti o l'esito di procedimenti penali; potrebbe mettere insieme informazioni che acquisisce su una persona senza che questa ne sia a conoscenza; potrebbe essere usata per creare "bolle" in rete per strumentalizzare l'informazione; potrebbe portare alla scomparsa di molti posti di lavoro, anche se ne verranno creati al tri e di migliori è cruciale che ci sia un'adeguata formazione; potrebbe portare a una distorsione della concorrenza con accumoli di informazioni; potrebbe portare a perdita di controllo sugli armamenti

Prosegue il Parlamento europeo nella sua valutazione anche dei potenziali benefici, potendo trovare soluzione a molteplici problematiche, quali ad esempio, in campo medico e in quello dell'istruzione,

sistemi di trasporto più sicuri, migliorare e rendere più sicura la manutenzione dei macchinari, offrire percorsi di vendita più ottimizzati e fluidi, risparmiare energia.

Riferimenti: proposta dell'Commissione europea del 21/04/2021

Maxi sanzione a IREN per violazione delle norme sul consenso degli interessati

A seguito di diversi reclami e segnalazioni, il Garante ha accertato che la società Iren Mercato Spa aveva trattato dati personali per attività di telemarketing non aveva raccolto direttamente, ma che aveva acquisito da altre fonti. Iren, infatti, aveva ottenuto liste di anagrafiche da una S.r.l., che a sua volta le aveva acquisite, in veste di autonomo titolare del trattamento, da altre due aziende. Queste ultime società avevano ottenuto il consenso dei potenziali clienti per il telemarketing effettuato sia da loro che da parte di terzi, ma tale consenso non copriva anche il passaggio dei dati dei clienti dalla S.r.l. all'Iren.

Il consenso, inizialmente rilasciato da un cliente ad una società anche per attività promozionali di terzi, non può estendere la sua efficacia anche a successive cessioni ad ulteriori titolari. Tali cessioni infatti non sarebbero supportate dal necessario consenso, specifico ed informato dell'interessato.Questo l'importante principio enucleato dal Garante che ha comminato una sanzione di circa 3 milioni di euro ad Iren Mercato S.p.A. per non aver verificato che tutti i passaggi dei dati dei destinatari delle promozioni fossero coperti da consenso.L'ammontare della sanzione applicata dal Garante, è stato motivato anche dal fatto che le liste anagrafiche, prive di tutti i consensi necessari e di cui il Garante ha vietato ogni ulteriore utilizzo a fini promozionali, riguardavano diversi milioni di persone. L'Autorità ha anche rivolto un avvertimento alla società per aver fornito una rappresentazione ed una documentazione probatoria incompleta ed inidonea durante l'istruttoria.

Riferimenti: provvedimento n. 192/2021; Newsletter GPDP n. 478/2021

Maxi sanzione a Glovo

Prima decisione del Garante riguardante i rider che fa seguito a un ciclo ispettivo sulle modalità di gestione dei lavoratori di alcune delle principali società di food delivery che operano in Italia.

Il Garante italiano ha anche attivato, per la prima volta, una operazione congiunta di cooperazione europea, ai sensi del Gdpr, con il Garante spagnolo (AEPD) per verificare il funzionamento della piattaforma digitale di proprietà della capogruppo GlovoApp23.

L'Autorità ha rilevato una serie di gravi illeciti, in particolare riguardo agli algoritmi utilizzati per la gestione dei lavoratori:
la società, ad esempio, non aveva adeguatamente informato i lavoratori sul funzionamento del sistema e non assicurava garanzie sull'esattezza e la correttezza dei risultati dei sistemi algoritmici utilizzati per la valutazione dei rider;
non garantiva nemmeno procedure per tutelare il diritto di ottenere l'intervento umano, esprimere la propria opinione e contestare le decisioni adottate mediante l'utilizzo degli algoritmi in questione, compresa l'esclusione di una parte dei rider dalle occasioni di lavoro.

La società Foodinho, controllata da GlovoApp23, dovrà modificare il trattamento dei dati dei propri rider, effettuato tramite l'utilizzo di una piattaforma digitale, e verificare che gli algoritmi di prenotazione e assegnazione degli ordini di cibo e prodotti non producano forme di discriminazione.

La società dovrà anche pagare una sanzione di 2,6 milioni di euro. Nel calcolare la sanzione di 2,6 milioni di euro alla società italiana Foodinho per i trattamenti illeciti effettuati, l'Autorità ha tenuto conto anche della limitata collaborazione offerta dalla società nel corso dell'istruttoria e dell'elevato numero di rider coinvolti in Italia, circa 19.000 al tempo dell'ispezione. La società spagnola GlovoApp23 è invece oggetto di un autonomo procedimento condotto dall'AEPD, con la collaborazione del Garante italiano.
Il Garante ha concesso a Foodinho 60 giorni di tempo per avviare le misure necessarie per correggere le gravi violazioni rilevate e ulteriori 90 giorni per completare gli interventi sugli algoritmi.

Riferimenti: Provvedimento GPDP n. 234/2021

Garante privacy: vietato il controllo indiscriminato sui lavoratori in ordine alla navigazione internet

Interessante pronuncia del Garante in materia di controllo dei lavoratori e impatti privacy.

La vicenda ha avuto avvio da un reclamo promosso verso l'Autorità garante da parte di un dipendente del Comune di Bolzano che, nel corso di un procedimento disciplinare, aveva scoperto di essere stato costantemente controllato. L'amministrazione, che inizialmente gli aveva contestato la consultazione di Facebook e Youtube durante l'orario di lavoro, aveva poi archiviato il procedimento per l'inattendibilità dei dati di navigazione raccolti.

Dagli accertamenti del Garante è emerso che il Comune impiegava, da circa dieci anni, un sistema di controllo e filtraggio della navigazione internet dei dipendenti, con la conservazione dei dati per un mese e la creazione di apposita reportistica, per finalità di sicurezza della rete.

Nell'ambito dell'istruttoria, sono state inoltre riscontrate violazioni anche in merito al trattamento dei dati relativi alle richieste di accertamento medico straordinario da parte dei dipendenti, effettuate attraverso un apposito modulo, messo a disposizione dall'amministrazione, che prevedeva la presa visione obbligatoria da parte del dirigente dell'unità organizzativa, circostanza che comportava un trattamento di dati sulla salute illecito.

Sebbene il datore di lavoro avesse stipulato un accordo con le organizzazioni sindacali, come richiesto dalla disciplina di settore, il Garante ha evidenziato che tale trattamento di dati deve comunque rispettare anche i principi di protezione dei dati previsti dal Gdpr.

Il sistema, implementato dal Comune, senza aver adeguatamente informato i dipendenti, consentiva invece operazioni di trattamento non necessarie e sproporzionate rispetto alla finalità di protezione e sicurezza della rete interna: effettuando una raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web visitati dai singoli dipendenti, raccoglieva informazioni estranee all'attività professionale e comunque riconducibili alla vita privata dell'interessato.

Questi i principi enunciati dal Garante:

- non è possibile monitorare la navigazione internet dei lavoratori in modo indiscriminato indipendentemente da specifici accordi sindacali;
- le eventuali attività di controllo devono comunque essere sempre svolte nel rispetto dello Statuto dei lavoratori e della normativa sulla privacy;
- l'esigenza di ridurre il rischio di usi impropri della navigazione in Internet non può portare al completo annullamento di ogni aspettativa di riservatezza dell'interessato sul luogo di lavoro, anche nei casi in cui il dipendente utilizzi i servizi di rete messi a disposizione del datore di lavoro.

Il Garante, tenendo conto della piena collaborazione dell'amministrazione, ha disposto una sanzione di 84.000 euro per l'illecito trattamento dei dati del personale. Il Comune dovrà anche adottare misure tecniche e organizzative per anonimizzare il dato relativo alla postazione di lavoro dei dipendenti, cancellare i dati personali presenti nei log di navigazione web registrati, nonché aggiornare le procedure interne individuate e inserite nell'accordo sindacale.

Riferimenti: provvedimento GPDP n. 190/2021; Newsletter n. 478/2021

Cookie: pubblicate le nuove Linee guida del Garante

Terminata la fase di consultazione, pubblicate in via definitiva le nuove Linee guida del Garante privacy sui cookie che hanno l'obiettivo di rafforzare il potere di decisione degli utenti riguardo

all’uso dei loro dati personali quando navigano on line. Il provvedimento è stato adottato tenendo conto degli esiti della consultazione pubblica promossa alla fine dello scorso anno.
I titolari dei siti avranno 6 mesi di tempo dalla pubblicazione in G.U. per conformarsi ai principi contenuti nelle Linee guida (entro il 9 febbraio 2022).
No a scrolling e a cookie wall se non in casi particolari, limiti alla reiterazione della richiesta di consenso.
Di seguito le principali indicazioni sull'uso dei cookie.

Informativa

L’informativa agli utenti dovrà indicare: anche gli eventuali altri soggetti destinatari dei dati personali; i tempi di conservazione delle informazioni; le modalità di esercizio dei diritti dell'interessato in particolare diritto di accesso e di reclamo all'Autorità; dovrà poter essere fruibile anche a persone con disabilità.
Potrà essere resa multilayer (su più livelli) anche su più canali (multichannel) e con diverse modalità (ad esempio, con pop up, video, interazioni vocali).
Resta confermato l’obbligo della sola informativa per i cookie tecnici, anche inserita nell’informativa generale. Il Garante raccomanda poi che i cookie analytics, usati per valutare l’efficacia di un servizio, siano utilizzati solo a scopi statistici.

Consenso

a) Il meccanismo di acquisizione del consenso on line dovrà innanzitutto garantire che, per impostazione predefinita, al momento del primo accesso ad un sito web, nessun cookie o altro strumento diverso da quelli tecnici venga posizionato all’interno del dispositivo dell’utente, né venga utilizzata altra tecnica di tracciamento attiva (ad esempio, cookie di terze parti) o passiva (ad esempio, il fingerprinting).
b) Per i cookie di profilazione rimane la necessità del consenso da richiedere attraverso un banner ben distinguibile sulla pagina web, attraverso il quale dovrà anche essere offerta agli utenti la possibilità di proseguire la navigazione senza essere in alcun modo tracciati, ad esempio chiudendo il banner cliccando sulla caratteristica X da inserire in alto a destra.
c) Scrolling: il Garante precisa che il semplice spostamento in basso del cursore (scroll down) non rappresenta una idonea manifestazione del consenso. I titolari dei siti (publisher) dovranno eventualmente inserire lo scrolling in un processo più articolato nel quale l’utente sia in grado di generare un evento, registrabile e documentabile presso il server del sito, che possa essere qualificato come azione positiva idonea a manifestare in maniera inequivoca la volontà di prestare un consenso al trattamento.
d) Cookie wall (sistema che vincola gli utenti all’espressione del consenso): il Garante chiarisce che questo meccanismo è da ritenersi illegittimo. Salva l’ipotesi, da verificare caso per caso, nella quale il titolare del sito consenta comunque agli utenti l’accesso a contenuti o servizi equivalenti senza richiesta di consenso all’uso dei cookie o di altri tracciatori.

e) Questione della ripresentazione del banner ad ogni nuovo accesso: il Garante precisa che tale prassi per la richiesta di consenso agli utenti che in precedenza l'abbiano negato, non trova ragione negli obblighi di legge e risulta una misura ridondante e invasiva. La scelta dell'utente dovrà essere debitamente registrata e non più sollecitata, a meno che: non mutino significativamente le condizioni del trattamento; sia impossibile sapere se un cookie sia già memorizzato nel dispositivo; siano trascorsi almeno 6 mesi. Fermo in ogni caso il diritto degli utenti di revocare in qualsiasi momento il consenso precedentemente prestato.
f) I publisher rendano manifesti nell'informativa almeno i criteri di codifica dei tracciatori adottati da ciascuno.

Riferimenti: provvedimento GPDP n. 231/2021 in G.U. n. 163 del 09/07/2021