



SCADENZA BANDI, QUESTIONE DI SECONDI

La domanda di partecipazione ad un bando pubblico inviata via PEC è ricevibile se le ricevute di accettazione e consegna riportano un orario di pochi secondi successivo a quello di scadenza indicato nel bando?

No, secondo il Consiglio di Stato (sent. n. 8546/2024) la domanda è irricevibile perché tardiva, anche se il ritardo è solo di pochi secondi.

Massima attenzione, pertanto, nella **verifica degli orari di invio delle domande a mezzo PEC**, al fine di scongiurare il rischio di esclusione per tardività.

PUBBLICATO SU: <https://www.dirittoegiustizia.it/#/documentDetail/11024111>



NIENTE SANZIONI PER LA VIOLAZIONE PRIVACY DI LIEVE ENTITÀ

In un recente provvedimento (n. 441/2024), il Garante della privacy italiano ha stabilito che non scattano automaticamente sanzioni in caso di violazioni della privacy derivanti da errori umani occasionali e di lieve entità.

Il caso riguarda due turisti e una multa "sbagliata". Nel valutarlo, l'Autorità ha qualificato l'accaduto come una violazione dei dati personali (data breach) dovuta ad un errore umano nella registrazione del noleggio. Tuttavia, considerando che si è trattato di un **disguido occasionale**, non imputabile a problemi informatici o di sistema, **prontamente rettificato dalla società**, il Garante ha deciso di chiudere il reclamo senza applicare misure correttive o sanzioni. Ha comunque invitato l'autonoleggio a vigilare costantemente sulle misure di sicurezza per prevenire simili errori umani.

PUBBLICATO SU, PREVIO LOGIN: <https://www.federprivacy.org/strumenti/accesso-ristretto/se-la-violazione-della-privacy-deriva-da-un-errore-umano-puo-non-scattare-la-sanzione>



ARGOMENTO E TEMI TRATTATI

da Paolo Anastasio nell'articolo "IT Wallet disponibile da oggi per tutti: tra i primi in Ue. Non serve scannerizzare i documenti: evviva l'interoperabilità dei dati": <https://www.key4biz.it/it-wallet-il-portafoglio-digitale-disponibile-da-oggi-quali-documenti-completare-e-come-funziona/514123/>

IT WALLET, DA OGGI DISPONIBILE TUTTI

Dal 4 dicembre, conclusa la fase di sperimentazione, l'IT Wallet, il portafoglio digitale italiano disponibile nell'app IO, è accessibile a tutti i cittadini maggiorenni. L'obiettivo è quello di renderlo operativo per l'intera popolazione entro il 2025, con l'intenzione di integrarlo, entro il 2026, nel portafoglio digitale europeo, Eudi Wallet, per facilitarne l'uso negli altri Paesi dell'Unione Europea.

La prima novità: non è necessario scannerizzare i documenti per caricarli; è sufficiente fornire il consenso per aggiungere la patente di guida, la carta europea della disabilità e la tessera sanitaria. L'inserimento della tessera sanitaria è avvenuto in modo immediato: l'app IO ha estratto i dati necessari dalla banca dati del MEF – Ragioneria Generale dello Stato, e in pochi secondi abbiamo già nel nostro IT Wallet la tessera sanitaria, completa del relativo certificato di autenticità.

Inoltre, è possibile cliccare su 'mostra documento' per visualizzare la tessera sanitaria nella sua interezza.

REFERTI VIA E-MAIL A PROVA DI COMPLIANCE,
COSA FARE?

Con il provvedimento n. 620 del 17 ottobre 2024, il Garante Privacy è tornato sul tema della refertazione online, ribadendo l'importanza di applicare le Linee Guida del 2009 – che stabiliscono precisi accorgimenti per l'invio dei referti online - come requisiti minimi di sicurezza ai sensi dell'art. 32 GDPR.

Il caso oggetto del provvedimento riguardava una società che aveva inviato un referto medico ad un indirizzo email errato, senza proteggere l'allegato con adeguate misure di sicurezza, come una password di accesso. Pur non essendosi concretizzata alcuna violazione effettiva della riservatezza dei dati, in quanto il destinatario aveva prontamente cancellato il messaggio senza aprirlo, il mancato rispetto delle Linee Guida ha comportato l'irrogazione di una sanzione amministrativa di 7.000 euro.



PUBBLICATO SU: <https://www.federprivacy.org/informazione/primo-piano/refertazione-on-line-il-garante-ribadisce-criteri-di-privacy-by-design>



PUBBLICATO SU: <https://www.anticorruzione.it/-/news.03.12.24>

(Decreto legislativo 23 dicembre 2022, n. 201).

Quando gli enti locali devono affidare un servizio pubblico locale, sono tenuti a pubblicare tempestivamente una serie di atti sul proprio sito istituzionale e a inviarli contemporaneamente all'ANAC, affinché siano resi disponibili in una sezione dedicata del portale e accessibili attraverso la struttura iniziale della Piattaforma Unica della Trasparenza.

PIATTAFORMA UNICA DELLA TRASPARENZA PER GLI ENTI LOCALI

Promossa dall'ANAC, la Piattaforma Unica della Trasparenza continua il suo percorso di semplificazione burocratica per supportare gli enti locali.

Tra i servizi che stanno ottenendo buoni risultati, spicca quello dedicato alla **Trasparenza dei servizi pubblici locali di rilevanza economica**. Questo servizio permette agli enti locali e alle autorità competenti di gestire e consultare, attraverso apposite maschere di inserimento e ricerca, i dati e i documenti richiesti dalla **normativa del 2022** sul riordino dei servizi pubblici locali di rilevanza economica

GEDI SOTTO LALENTE DEL GARANTE

Il Garante privacy italiano ha emesso un avviso formale al Gruppo Editoriale Gedi riguardo all'accordo stipulato il 24 settembre con OpenAI. Questa intesa, che prevede la condivisione dei contenuti editoriali degli archivi digitali del gruppo, potrebbe comportare **rilevanti rischi per la privacy** di milioni di individui.

PUBBLICATO SU: <https://www.dimt.it/news/garante-privacy-avverte-gedi-rischi-nel-condividere-dati-personali-con-openai/>

COMUNI E IMPOSTA DI BOLLO, COME FARE?

I Comuni possono adempiere all'obbligo di pagamento dell'imposta di bollo in diversi modi. Oltre ai tradizionali **sportelli fisici** dove i cittadini possono presentare le proprie richieste, sono sempre più disponibili servizi digitali che consentono ai cittadini di svolgere le stesse operazioni utilizzando **SPID o CIE**.

Le principali normative di riferimento in materia sono il **D.P.R. 445 del 2000** (Testo Unico sulla Documentazione Amministrativa), il **CAD** e, in particolare, il **D.P.R. 642 del 1972** (Disciplina dell'imposta di bollo).

Nell'articolo viene presentata una panoramica delle regole, dei sistemi disponibili e dei dettagli da tenere in considerazione.

ARGOMENTO E TEMI TRATTATI da Giacomo Fioroni, nell'articolo "Imposta di bollo per i Comuni, come assolvere all'obbligo: tutti i metodi": <https://www.agendadigitale.eu/documenti/imposta-di-bollo-per-i-comuni-come-assolvere-allobligo-tutti-i-metodi/>



ARGOMENTO E TEMI TRATTATI da Antonella Salerno, nell'articolo "Cittadinanza digitale, in Toscana la prima legge regionale ad hoc": <https://www.corrierecomunicazioni.it/pa-digitale/cittadinanza-digitale-in-toscana-la-prima-legge-regionale-ad-hoc/>

CITTADINANZA DIGITALE, IN TOSCANA LA PRIMA LEGGE REGIONALE AD HOC

La Toscana è la prima regione italiana ad approvare una legge che regola l'**innovazione digitale e protegge i diritti dei cittadini**, anche alla luce delle nuove esigenze di transizione digitale delle PA.

Con il voto positivo del Consiglio Regionale, il provvedimento – che accorpa in un unico testo le due leggi precedenti che disciplinavano il settore – si allinea alle direttive dell'**Agenda Digitale Europea** e al **programma Europa Digitale**, oltre a considerare tutte le normative intervenute nel tempo riguardanti questo ambito.

Nel testo non si fissano solo dei principi riguardanti l'uso dell'intelligenza artificiale, ma si rafforzano anche quelli relativi alla **cybersicurezza** e al supporto al digitale per gli enti locali.

BANCHE DATI PIÙ PROTETTE CON LE LINEE GUIDA ACN

Fondamentali le **nuove Linee Guida** pubblicate dall'Agenzia per la cybersicurezza nazionale, poiché affrontano il **rischio di accessi non autorizzati**, sia da parte di minacce interne (insider threats) che esterne. Questo documento offre un quadro esaustivo delle **normative vigenti**, incluse quelle stabilite dal **DL 105/2019** riguardante il Perimetro di sicurezza nazionale cibernetica, accompagnato da esempi pratici per una corretta implementazione operativa. Viene posta particolare enfasi sulla gestione dei rischi legati alla supply chain, sul controllo degli accessi privilegiati, sulla **formazione del personale amministrativo** e sulle attività di monitoraggio e auditing interno. Questo documento si colloca all'interno della più ampia **Strategia nazionale di sicurezza cibernetica**, volta a potenziare la resilienza dello spazio digitale italiano attraverso misure tecniche, organizzative e procedurali rivolte principalmente ai soggetti pubblici e privati che rientrano nel Perimetro nazionale di sicurezza cibernetica. In questo contesto, l'ACN svolge un ruolo di supporto e vigilanza per garantire l'aderenza alle normative e per migliorare la sicurezza complessiva.



PUBBLICATO SU: <https://www.key4biz.it/rafforzamento-della-protezione-delle-banche-dati-acn-pubblica-le-linee-guida/513206/>



CYBERSECURITY: E SE APPLICASSIMO UN FRAMEWORK ZERO TRUST ANCHE NEI SISTEMI PUBBLICI?

I comuni italiani detengono un ampio insieme di dati sensibili riguardanti i cittadini, che spaziano dai servizi anagrafici ai documenti di stato civile. In un modello di sicurezza tradizionale basato sul perimetro, un dipendente avrebbe la possibilità di accedere a tali informazioni con una sola autenticazione all'inizio della sua sessione lavorativa.

Come aumentare la sicurezza interna ed esterna, al fine di ridurre il rischio di accessi non autorizzati e rendere più difficile la propagazione di attacchi all'interno della rete?

Il **modello Zero Trust** rappresenta una strategia di sicurezza della rete che si fonda sull'idea che l'accesso ai carichi di lavoro o ai sistemi IT di un'azienda, sia da parte di utenti o dispositivi interni che esterni, deve essere autorizzato esclusivamente quando è considerato strettamente necessario. In altre parole, non si basa su una fiducia presunta.

ARGOMENTO E TEMI TRATTATI da Andrea Rossetti nell'articolo "Cybersecurity, come applicare un framework zero trust anche nei sistemi pubblici?": <https://www.key4biz.it/cybersecurity-come-applicare-un-framework-zero-trust-anche-nei-sistemi-pubblici/511598/>