pentha
Servizi Integrati per le Impresa
ANNO 14 NUMERO 255

Aderente ASSO DPO Associazione Data Protection Officer

FEDERPRIVACY Federazione Italiana Privacy
Delegazione provinciale

Newsletter

Cuneo, 31/08/2021

In questo numero

Il focus di questo numero

Gentili Lettori,

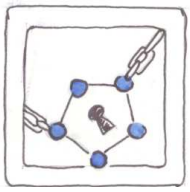
torniamo operativi dopo la tradizionale pausa estiva con l'augurio che la parte finale di questo 2021 possa essere migliore della prima.

Tiene banco a livello privacy, e non solo, la vicenda "green pass" con il Garante impegnato su più fronti come documentato dalle news contenute all'interno.

Interessante sarà anche seguire l'evoluzione della nuova Legge sulla Privacy in Cina, dove gli aspetti "ossimorici" non mancheranno di certo.

Infine un monito a tutti i possessori di impianti di Videosorveglianza: la verifica del rispetto delle varie norme privacy/giuslavoristiche sarà oggetto dei controlli del Garante per questo secondo semestre 2021.

Lo staff di Pentha Vi augura una buona lettura!



Controlli sugli impianti di videosorveglianza

L'angolo della privacy

Videosorveglianza e data breach sotto la lente del Garante Privacy

Meglio non trascurare le regolarità dei sistemi di videosorveglianza pubblici e privati, valutando attentamente la base giuridica del trattamento, la durata della conservazione delle immagini, le informative, e facendo particolare attenzione ai data breach e al trattamento eventuale di dati biometrici. Con deliberazione 22 luglio 2021 [doc.web 9689657], lo ha chiarito il Garante per la protezione dei dati personali, che ogni semestre fornisce indicazioni generali sui controlli da effettuare di propria iniziativa o tramite il Nucleo Speciale Privacy e Frodi Telematiche della Guardia di finanza. Per il secondo semestre del 2021 sotto osservazione saranno soprattutto gli impianti di videosorveglianza pubblici e privati. In particolare quelli che trattano dati biometrici per il riconoscimento facciale.

Anche la videosorveglianza aziendale richiede quindi l'installazione di un cartello con tutte le informazioni minime ed il rinvio ad una idonea informativa di secondo livello che può essere pubblicata anche sul sito web aziendale oppure fornita in modalità ordinarie, come ha chiarito lo stesso Garante con l'ordinanza ingiunzione n. 191 del 13 maggio 2021, in cui il nucleo tutela del lavoro dei carabinieri di Ferrara ha accertato il posizionamento di alcune telecamere all'interno di un'azienda senza il posizionamento in loco di alcun cartello o informativa.

Al ricevimento della segnalazione il Garante ha attivato una procedura sanzionatoria che si è conclusa con l'applicazione di una sanzione amministrativa. L'art. 13 del regolamento europeo n. 679/2016, il Gdpr, prevede l'applicazione di un cartello sintetico con rinvio ad informazioni di dettaglio sulle finalità del trattamento e sui diritti dell'interessato. In considerazione della particolare attenzione che il Garante pone sui sistemi di videosorveglianza, nell'ultima parte del 2021 Federprivacy ha promosso due eventi formativi dedicati a questi delicati temi, rispettivamente il "Corso La videosorveglianza con le Linee Guida EDPB 3/2019" di quattro ore in agenda per il 25 settembre, e anche il "Corso Specialistico per Privacy Officer nel settore Videosorveglianza" di 16 ore, con lezioni di quattro ore ciascuna in programma il 14, 21, 28 ottobre e l'ultima il 4 novembre.

Oltre gli impianti di videosorveglianza, nel secondo semestre del 2021 sotto la lente dell'Autorità vi saranno anche i trattamenti effettuati dalle società di marketing e di profilazione, dai data broker e dalle banche dati reputazionali, e anche i trattamenti effettuati dagli istituti di ricovero e cura e dalle società rientranti nel settore del food delivery e ai data breach.

Fonte: Federprivacy.it

Cina: approvata una nuova legge sulla privacy

La protezione dei dati personali in un regime post comunista basato sul modello capitalista

Secondo quanto riportato dai media statali filogovernativi, la Cina ha approvato una nuova legge sulla privacy per proteggere i dati personali degli utenti, entrerà in vigore dal 1° novembre 2021. Ecco cosa prevede:

La normativa, formalmente ribattezzata "Legge sulla protezione delle informazioni personali", è stata approvata dal legislatore cinese venerdì 20 agosto secondo quanto riferito da Reuters, e chiede alle aziende di ottenere il consenso degli utenti prima di raccogliere dati personali oltre a regolamentare le modalità atte a garantire la protezione dei dati quando vengono fatti uscire dal Paese.

Le aziende tecnologiche che gestiscono informazioni e dati personali, stando al nuovo quadro normativo deciso dal governo locale, devono avere una persona designata incaricata di sovrintendere alla loro protezione, oltre a condurre controlli regolari per assicurarsi che rispettino le regole.

Inoltre, secondo Reuters, le società che gestiscono i dati personali degli utenti avranno necessità di dimostrare di avere uno scopo chiaro e ragionevole per farlo, limitandosi peraltro allo "scopo minimo necessario per raggiungere gli obiettivi" derivati dal trattamento dei dati in questione.

In un editoriale sul giornale statale cinese People's Court Daily, l'Assemblea nazionale del popolo ha lodato la nuova legislazione. "La personalizzazione è il risultato della scelta di un utente e le vere raccomandazioni personalizzate devono garantire la libertà di scelta dell'utente, senza costrizioni", recita in fatti l'editoriale pubblicato.

Aggiungendo che, "pertanto, agli utenti deve essere concesso il diritto di non utilizzare funzioni di raccomandazione personalizzate". Un piccolo passaggio democratico in un Paese che, sotto la guida di Xi Jinping, ha confermato di essere un regime e nulla più, anche se evidentemente post-comunista e basato sul modello capitalista di società.

Fonte: Federprivacy.it

Green pass per l'accesso agli uffici pubblici, il Garante della Privacy invita la Regione Siciliana a stop ordinanza

Il Garante richiama al rispetto della gerarchia delle fonti del diritto

Il Garante per la protezione dei dati personali ha inviato alla Regione Siciliana una richiesta di informazioni in merito alle nuove modalità per l'accesso degli utenti agli uffici pubblici e agli edifici aperti al pubblico introdotte dall'ordinanza presidenziale del 13 agosto 2021, n. 84, nell'ambito delle misure di contrasto della pandemia da Covid19.

L'ordinanza prevede che le persone sprovviste della certificazione verde non possono accedere agli uffici pubblici e agli edifici aperti al pubblico e possono usufruire dei servizi, anche di quelli resi da privati preposti all'esercizio di attività amministrative, esclusivamente in via telematica, o comunque da remoto.

Le misure di sanità pubblica che implichino il trattamento di dati personali - ricorda l'Autorità - ricadono nelle materie assoggettate alla riserva di legge statale e, pertanto, non possono essere introdotte con un'ordinanza regionale, ma solo attraverso una disposizione di rango primario, previo parere del Garante.

Non risulta, inoltre, che i più recenti interventi normativi in tema di certificazioni verdi abbiano imposto l'esibizione di tali documenti per l'accesso dell'utenza agli uffici pubblici o similari, per cui il loro utilizzo per finalità ulteriori e con modalità difformi rispetto a quanto previsto dalla legge statale creerebbe una evidente disparità di trattamento a livello territoriale.

Il Garante privacy quindi, oltre a chiedere chiarimenti ha invitato la Regione - già destinataria di un "avvertimento" sui trattamenti di dati personali relativi allo stato vaccinale dei dipendenti pubblici - a sospendere l'efficacia di tali misure nell'ipotesi in cui siano già state messe in atto, circoscrivendo l'uso delle certificazioni verdi ai soli casi individuati dalle disposizioni di legge statali.

Fonte: Federprivacy.it

Pasticcio Green Pass: la Regione Toscana diffonde un valido QR Code impossibile da revocare e acquistabile online per pochi euro

Per i furbetti del Green Pass non c'è bisogno di andare nel Dark Web o su qualche canale Telegram di truffatori per procurarsi un valido QR Code pagando centinaia di euro, perché si può comprare con pochi click a 9,99 euro su Alamy, noto sito di vendita online di immagini in stock.

E a quanto pare il fotografo che lo ha messo in vendita online, pur avendo provveduto a cancellare le proprie generalità nella foto pensando così di tutelare la propria privacy, non si è però fatto troppo domande su quel QR Code che potrebbe sembrare un piccolo ed innocuo geroglifico quadrato, ma che in realtà contiene varie informazioni personali di natura sensibile, e che è facilmente decifrabile da qualunque curioso o malintenzionato.

E neanche tale fotografo deve aver prestato attenzione alle raccomandazioni di Guido Scorza, componente del Garante per la protezione dei dati personali, che nelle scorse settimane aveva spiegato che il Green Pass deve essere ben custodito e mostrato solo alle forze dell'ordine e ai soggetti autorizzati ad effettuare i controlli, resistendo alla tentazione di condividere il proprio QR Code su social e siti web.

Ma se il professionista è stato senza dubbio maldestro ad utilizzare il proprio QR Code per realizzare una foto destinata ad essere poi commercializzata su larga scala, rischiando così che innumerevoli imbroglioni possano sfruttare la sua identità per accedere liberamente a concerti ed eventi sportivi, una gaffe ancor peggiore l'ha però commessa la Regione Toscana, che il 4 agosto scorso ha incautamente usato proprio quell'immagine postandola nelle sui propri profili social diffondendola ai suoi 20.000 follower su Twitter e agli oltre 160.000 seguaci della sua pagina Facebook istituzionale.

Se è vero che l'occasione fa l'uomo ladro, ovviamente la Regione Toscana quando è venuta a conoscenza dell'involontario assist che aveva fatto agli aspiranti falsari è corsa subito ai ripari cancellando l'immagine incriminata, ma sta di fatto che nel frattempo migliaia di utenti l'avevano già condivisa con i propri contatti, e in ogni caso il Web non dimentica, perché una copia cache della foto del QR Code è sempre recuperabile attraverso uno qualsiasi dei siti di archiviazione di contenuti online che ogni giorno scansionano e copiano miliardi di pagine su internet.

E come se tutto ciò non bastasse, a fare una scoperta allarmante è stato Matteo G.P. Flora, professore in Corporate Reputation & Business Storytelling ed in Data Driven Strategies, che in un approfondito videoclip pubblicato su Youtube ha dimostrato che quel QR Code accidentalmente diffuso dalla Regione Toscana, come del resto tutti quelli dei Green Pass regolarmente ottenuti da milioni di italiani, non sono in nessun caso invalidabili,

neanche in caso di frode, divulgazione accidentale, o di accertamento di positività da Covid-19 di una persona precedentemente vaccinata o guarita, perché non esiste una banca dati dei Green Pass revocati, ed è quindi tecnicamente impossibile annullarli prima della sua naturale scadenza che avviene trascorsi 9 mesi dalla sua emissione.

Da ciò ne deriva, che sebbene il Ministero dell'interno abbia chiarito che i ristoratori e i titolari delle altre attività che devono controllare il Green Pass dei loro clienti sono tenuti a chiedere il documento d'identità del cliente solo "quando appaia manifesta l'incongruenza con i dati anagrafici contenuti nella certificazione", alla luce dell'improvvida diffusione di QR Code validi da parte della Regione Toscana e da altri soggetti che hanno condotto inavvertitamente attività analoghe usando immagini incautamente comprate negli store e realizzate da professionisti sprovveduti, adesso il numero dei potenziali falsi si moltiplica a dismisura, e per avere certezza che chi presenta il Green Pass ne sia anche il legittimo intestatario all'esercente non rimarrebbe altro che procedere al controllo a tappeto dei documenti d'identità di tutti gli avventori.

Fonte: Federprivacy

Green pass, il Garante Privacy non pone veti sul controllo dei documenti d'identità da parte dei gestori di bar e ristoranti

Controlli sull'identità in assenza di raccolta di dati

Controllare il green pass significa non solo utilizzare specifici canali digitali (l'App VerificaC19 messa a punto dal governo) per la lettura delle certificazioni verdi, ma anche verificare l'identità del titolare. In attesa che arrivi la circolare promessa dal Viminale con le indicazioni per gli esercenti e i gestori dei servizi, il Garante privacy sconfessa il ministro dell'interno Luciana Lamorgese che lunedì aveva dichiarato di voler esonerare bar e ristoranti dal controllo dei documenti di identità dei clienti muniti di green pass.

Rispondendo a un quesito della regione Piemonte, l'Autorità presieduta da Pasquale Stanzione, ha confermato la tesi, suffragata dalla lettera del dpcm 17 giugno, (quello che ha indicato le specifiche tecniche per i controlli del green pass) dell'impossibilità di controllare la titolarità delle certificazioni senza un contestuale accertamento dell'identità di chi le presenta.

«La disciplina procedurale, riconducibile al dpcm 17 giugno 2021», scrive il Garante all'assessore della regione Piemonte Maurizio Marrone, «comprende, oltre la regolamentazione degli specifici canali digitali funzionali alla lettura della certificazione verde, anche gli obblighi di verifica dell'identità del titolare della stessa, con le modalità e alle condizioni di cui all'art. 13, comma 4, del citato dpcm».

Il Garante ha confermato che non esistono problemi di trattamento dei dati personali nella disciplina del green pass, proprio perché lo stesso dpcm 17 giugno, all'articolo 13 comma 5 esclude la raccolta «da parte dei soggetti verificatori, dei dati dell'intestatario della certificazione, in qualunque forma». Secondo l'Authority il trattamento dei dati personali è consentito nella misura in cui si limita alla mera verifica dell'identità dell'intestatario della certificazione verde, mediante richiesta di esibizione di un documento.

Fonte: Federprivacy

Attacco hacker a Tim: cosa rischiano i clienti e cosa fare

Cambio di password nell'area "MyTim"

Tim è stata colpita da un attacco hacker che ha messo a rischio la sicurezza dei dati dei suoi clienti. La notizia arriva direttamente dall'azienda che ha prontamente provveduto ad informare i suoi utenti attraverso una mail spiegando anche come difendersi. Nello specifico le azioni fraudolente, attuate da ignoti, avrebbero messo a rischio le credenziali di accesso della sezione MyTIM, ossia la pagina riservata ai clienti in cui è possibile controllare lo stato del proprio contratto e le varie bollette.

Con una mail inviata ai suoi clienti, Tim ha fatto sapere di essere stata vittima di un attacco hacker. Nella comunicazione infatti viene riportato che "a fronte delle attività di controllo di sicurezza sui nostri sistemi, sono state rilevate attività anomale, svolte da parte di soggetti terzi ignoti, che potrebbero mettere a rischio la riservatezza delle tue credenziali di accesso a MyTIM".

La minaccia dell'attacco è dimostrata anche dal fatto che TIM abbia fatto sapere di aver informato le autorità competenti in materia, ritenendosi parte lesa tanto quanto i clienti. L'azienda tuttavia esclude la possibilità che i dati trafugati possano essere utilizzati per abilitare funzioni di pagamento, comunque viene precisato che potrebbero essere utilizzati per tentativi di phishing.

Come spesso accade in queste situazioni i rischi maggiori che corrono gli utenti sono il possibile "accesso da parte di terzi a servizi online ai quali ti sei registrato, con conseguente perdita di controllo sui tuoi dati personali, possibile acquisizione fraudolenta di informazioni che ti riguardano o anche eventuali situazioni di furto di identità". Proprio per questo motivo Tim ha deciso di "disabilitare in via precauzionale le tue credenziali MyTIM, rendendo obbligatorio il cambio password al primo accesso all'Area privata MyTIM".

In sostanza tutti gli utenti coinvolti nel breach dovranno modificare la loro password. Tim suggerisce inoltre di "non utilizzare più la vecchia password, né una simile, nonché di modificare la password utilizzata per l'accesso a qualsiasi altro servizio online, qualora coincidente o simile a quella precedentemente utilizzata su MyTIM".

Nella mail inviata ai suoi clienti, l'azienda ha ricordato inoltre che per prevenire abusi o frodi è sempre consigliabile utilizzare password "strutturate", ossia composte da lettere, numeri e caratteri speciali, che devono essere modificate periodicamente. Inoltre Tim invita a fare attenzione alle attività di phishing e ad utilizzare un buon antivirus.

Fonte: Federprivacy

K.O. il fascicolo sanitario elettronico della Regione Lombardia

Tempi duri per gli IT regionali

A differenza di quanto è toccato in sorte alla Regione Lazio, stavolta pare (ma è tutto da dimostrare) che non sia colpa degli hacker se i sistemi informativi della sanità regionale lombarda sono andati fuori uso. Il portale che eroga i servizi essenziali tra cui quello del fascicolo sanitario elettronico non è infatti raggiungibile dalla vigilia di ferragosto. Nessuna azione terroristica – come invece temuto a Roma da Zingaretti e D'Amato – ma semplicemente una défaillance determinata da un problema dei sistemi di climatizzazione che garantiscono la temperatura idonea a permettere il regolare funzionamento di server e computer del Centro Elaborazione Dati.

Mentre i più sarcastici fanno notare che – ironia della sorte – la società che gestisce questo genere di attività si chiama "Aria" (e forse ci sarebbe voluto un salvifico "condizionata" ad assicurare l'efficienza dell'opera prestata), i più clementi fanno osservare che certi imprevisti possono capitare in sorte un po' a tutti.

In questa stagione, infatti, è difficile immaginare che possa fare caldo e quindi il mantenimento in efficienza di certi impianti è proprio l'ultimo pensiero anche dei più previdenti manager. A ferragosto poi è pressoché impensabile ipotizzare l'arrivo di afa e canicola…

Aria S.p.A. aveva subito garantito che il disservizio era in fase di risoluzione e nel frattempo già c'era chi immaginava i dipendenti del "Pirellone" armati di ventagli e ventilatori per dare sollievo ai fumanti apparati informatici. Il personale più allineato politicamente aveva suggerito anche la distribuzione di mojito da caricare sui sistemi tramite porta USB o altre periferiche opportunamente dotate di ombrellino da cocktail.

Ogni commento è ragionevolmente superfluo.

I pirati informatici – se possibile – sono pregati di eseguire un upload fraudolento di "senso della vergogna" direttamente sui dispositivi dei responsabili dei disastri tecnologici che stanno affliggendo la povera Italia delle malandate istituzioni pubbliche.

Nel frattempo il nostro applauso va a chi è riuscito in una simile impresa, restando in attesa che qualcun altro riesca addirittura a fare qualcosa di ancor più eclatante per rallegrare l'estate 2021

Fonte: Federprivacy

Francia, sanzionato 'Le Figaro' per violazione sui cookie

Regole sui cookies spesso disattese

Il quotidiano francese "Le Figaro" è stato sanzionato per 50.000 euro dall'autorità di controllo per la protezione dei dati nazionale (CNIL) a seguito di alcune segnalazioni ricevute per cui il sito web del noto editore avrebbe installato cookie pubblicitari di terze parti sui dispositivi degli utenti senza il loro consenso, e che quindi sarebbero stati profilati a loro insaputa.

La Commission Nationale de l'Informatique et des Libertés ha così imposto le sanzioni dopo che gli accertamenti condotti tra il 2020 e il 2021 avevano rivelato che effettivamente i cookie venivano automaticamente posizionati sui computer dei visitatori del sito lefigaro.fr, senza che venissero avvisati o chiedendo alcun consenso.

Data la quantità di dati personali che spesso raccolgono i cookie, il GDPR richiede che i siti web acquisiscano il consenso degli utenti prima che essi vengano installati su computer e dispositivi degli utenti.

Sempre a norma del Regolamento europeo sulla protezione dei dati personali, i siti web sono inoltre tenuti a gestire e rispettare l'eventuale rifiuto che gli utenti devono essere messi in grado di esprimere.

La "Société du Figaro" ha quindi violato le regole del Gdpr in quanto "non garantiva sistematicamente la raccolta del consenso". Come sottolinea il network di informazione Euractiv, la sanzione a Le Figaro non è che l'ultima di una serie di provvedimenti comminati dalla CNIL per violazioni della protezione dei dati, alcune delle quali sono state imposte per milioni di euro ai giganti del Web.

Fonte: Federprivacy

Oscuramento dati personali in una sentenza ammissibile solo per validi motivi

"Oscuramento" non sempre ammissibile

La Cassazione spiega che per ottenere l'oscuramento dei dati da una sentenza occorrono buoni motivi come la delicatezza della materia o la presenza di dati sensibili. Alla suprema Corte, adita per risolvere una questione di natura tributaria, viene chiesto anche, in via preliminare, di ottenere l'oscuramento dei nomi dalla sentenza. Gli Ermellini nel caso di specie non accolgono l'istanza perché la questione non verte su questioni delicate e nel provvedimento non è necessario indicare dati sensibili. Queste le conclusioni contenute nell'ordinanza n. 22561/2021 della Cassazione.

Due soggetti stipulavano un atto di compravendita immobiliare e al notaio l'ufficio territoriale dell'Agenzia delle Entrate notificava un avviso di liquidazione con cui gli venivano richieste maggiori imposte di registro, ipotecaria e catastale.

L'avviso veniva impugnato dal notaio, che affermava l'applicazione dell'aliquota agevolata visto che l'immobile oggetto del rogito, compreso il lastrico, in quanto pertinenza, costituiva una prima casa. Il ricorso venica accolto, ma a qual punto l'Agenzia ricorreva in appello e l'impugnazione veniva accolta dalla CTR.

Il notaio e i contribuenti ricorrevno allora in Cassazione, affidandosi a un unico motivo con cui deducono la violazione della nota II bis punto 3 art. 1 della tariffa , osservando che la menzione delle categorie catastali C2, C6 e C7 non significava che i beni classificati in altre categorie non potessero considerarsi pertinenze perché in questo caso era necessario fare riferimento all'art. 817 c.c.

Prima però facevano istanza per ottenere l'omissione dei dati dalla sentenza nel caso in cui venga comunicata a terzi ai sensi dell'art. 52 del Dlgs n. 196/2003.

La Cassazione si esprimeva in via preliminare sulla richiesta di oscuramento dei dati, riconoscendo la sussistenza di questo diritto, precisando però che la domanda di oscuramento "deve essere specificamente proposta e anche essere sostenuta dalla indicazione dei motivi legittimi che la giustificano, motivi che la parte deve specificare."

Motivi di cui il giudice è tenuto a vagliare la legittimità. Costui deve infatti valutare se le ragioni addotte sono meritevoli di accoglimento. La norma che prevede tale diritto non indica i motivi che giustificano tale richiesta, per cui ogni volta è necessario bilanciare le esigenze di riservatezza del singolo con il principio generale di conoscibilità degli atti giudiziari in forma completa, nel rispetto del principio d'informazione giuridica, espressione di democrazia.

Il Garante Privacy inoltre, con le linee guida del 2 dicembre 2010, ha stabilito che rappresentano motivi legittimi ai fini della

cancellazione dei propri dati da un provvedimento giudiziario, la natura "sensibili" dei dati in esso contenuti o la particolare delicatezza delle questioni trattate.

Passando quindi al caso di specie la Cassazione rileva come le parti, nel formulare detta richiesta, non hanno indicato i motivi legittimi posti alla base dell'istanza di oscuramento dei dati.

In una controversia tributaria in cui la questione centrale è rappresentata dalla diversa interpretazione di una norma di legge, non è presente alcun dato sensibile né la materia è così delicata da incidere su diritti personalissimi. Non sussiste neppure il rischio di compromettere l'onore o la reputazione delle parti che si sono limitati a dissentire su una norma, con un motivo, tra l'altro, fondato.

Il motivo infatti sollevato dal contribuente e dal notaio viene accolto dalla Cassazione, che da seguito al principio per il quale "in tema di imposta di registro, ai fini dell'estensione dell'aliquota agevolata per l'acquisto della prima casa, deve intendersi compreso tra le pertinenze dell'immobile (…) anche il lastrico solare di proprietà esclusiva dell'acquirente, senza che rilevi che il bene sia censito unitamente all'immobile principale, né che l'acquisto della pertinenza sia concluso con atto separato, assumendo la norma tributaria, nel riferimento alle unità immobiliari di classificazione catastale C2, C6 e C7 mera valenza complementare rispetto alla citata mozione civilistica."

Fonte: Federprivacy

Il cliente che registra di nascosto l'avvocato che parla male del collega non viola il Codice Privacy, e il file audio è utilizzabile in giudizio

Difendere un diritto in giudizio: vale la registrazione

Avvocato che parla male del collega incastrato dalla registrazione effettuata di nascosto dal cliente nello studio legale. Il file audio è utilizzabile nel processo civile in quanto riproduzione meccanica ex art. 2712 del Codice Civile né l'uso è precluso dal Codice Privacy: anche nel penale, infatti, la registrazione eseguita all'insaputa dell'interlocutore da una persona che è presente alla conversazione costituisce una prova documentale non costituisce un'intercettazione e dunque resta fuori dal campo delle garanzie ad hoc. Lo stabiliscono le s.u. civili della Cassazione con la Sentenza 20384/21.

Diventa definitiva la censura inflitta al professionista per una serie di condotte, fra le quali le espressioni offensive indirizzate all'ex collaboratore. All'uomo che sta registrando il colloquio col legale con un microregistratore nascosto l'avvocato propone di farsi restituire l'incartamento delle vertenze patrocinate dal collega e offre perfino all'interessato un posto di lavoro: cerca così di acquisire un cliente in modo non conforme a correttezza e decoro.

Decisivo ai fini della sanzione disciplinare il cd su cui finiscono le parole dell'incolpato verso l'ex collaboratore, accusato dal dominus di essere incapace e irriconoscente. Ma che evidentemente era d'accordo con l'autore della registrazione. Il file risulta utilizzabile perché nel penale, ad esempio, la registrazione audio realizzata da chi è legittimato ad assistere al colloquio non lede i diritti fondamentali dell'individuo tutelati dalla Costituzione: è quindi prova documentale utilizzabile in dibattimento ex articolo 234 Codice di Procedura Penale e non intercettazione ambientale soggetta alle garanzie ex articolo 266 CPP e seguenti.

Lo stesso Codice Privacy ne consente l'utilizzo se serve a far valere o difendere un diritto in giudizio. La registrazione effettuata nello studio legale è legittima per il Cnf che sul punto si limita a richiamare la motivazione del Consiglio distrettuale di disciplina. E il disconoscimento può trovare ingresso soltanto se l'incolpato prova che la realtà dei fatti non risponde a quella riprodotta.

Fonte: Federprivacy

Whistleblowing, sanzioni fino a 50.000 euro chi ostacola le denunce

Sanzioni a chi mette il bavaglio al "wistleblowing"

Sanzioni fino a 50.000 euro a tutela degli informatori su illeciti aziendali. È quanto prevede lo schema di decreto legislativo che recepisce la direttiva comunitaria del 2019 di riforma del whistleblowing. Le misure, inedite, saranno inflitte da Anac in una "forchetta" da 5.000 a 30.000 euro, quando accerta che sono state tenute condotte vessatorie o adottate misure ritorsive o quando verifica che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza; la sanzione sarà invece compresa tra un minimo di 10.000 euro e un massimo di 50.000, quando l'Autorità anticorruzione accerta che non sono state adottate procedure per l'inoltro e la gestione delle segnalazioni oppure che l'adozione delle procedure non è conforme a quanto stabilito dal decreto e anche quando non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute.

Va infatti ricordato che le segnalazioni interne, quelle cioè non indirizzate direttamente all'Anac, sono effettuate in forma scritta, anche con modalità informatiche, oppure orale, mediante canali progettati, realizzati e gestiti per garantire la riservatezza dell'identità della persona segnalante e del contenuto delle segnalazioni e della relativa documentazione e la protezione degli eventuali terzi citati nella segnalazione, anche ricorrendo a strumenti di crittografia, per impedire l'accesso da parte del personale non autorizzato. Le segnalazioni orali sono possibili attraverso linee telefoniche o attraverso altri sistemi di messaggistica vocale o, su richiesta della persona segnalante, attraverso un incontro diretto entro un termine ragionevole.

I soggetti cui devono essere indirizzate le segnalazioni (per esempio ilo responsabile anticorruzione nel settore pubblico, e l'organismo di vigilanza, nelle imprese che adottano modelli 231) sono obbligati, sottolinea il decreto, a rilasciare alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla presentazione ed entro tre mesi dall'avviso di ricevimento della segnalazione o, in mancanza, entro tre mesi dalla scadenza del termine di sette giorni dalla segnalazione forniscono riscontro.

Il decreto dettaglia poi anche gli atti ritorsivi rigorosamente vietati che vanno dal licenziamento (con l'equiparazione del mancato rinnovo o risoluzione anticipata del contratto a termine) e mancata promozione, sino a misure più sottili ma non meno insidiose come l'annullamento di un contratto di fornitura (il decreto copre anche soggetti formalmente terzi), l'inserimento in black list, l'annullamento di licenze o permessi, la sottoposizione a visite mediche o accertamenti psichiatrici.

Fonte: Federprivacy

Pentha Memo…

Memorandum sulle scadenze privacy, iniziative, eventi e servizi curati da Pentha e dalla rete di collaboratori (non è quindi esaustivo di tutti gli adempimenti contabili, fiscali, previdenziali e societari obbligatori).

Per ulteriori informazioni siamo a completa disposizione ai recapiti in calce.

Data scadenza	Descrizione
On demand	Corsi di formazione sul Regolamento Europeo Gdpr 2016/679

Pentha s.r.l. Servizi Integrati per le Imprese
Via Gobetti, 37 – 12100 Cuneo
Telefono 0171 489095 – Fax 0171 631346
Web www.pentha.eu Mail pentha@pentha.eu

http://www.facebook.com/pages/Pentha-srl-Servizi-Integrati-per-le-imprese/89151469538