CYBERSECURITY360

05/02/2021 16:17
Sito Web

cybersecurity360.it

TuPassi: perché la sanzione del Garante privacy è un monito per gli sviluppatori software

LINK: https://www.cybersecurity360.it/legal/privacy-dati-personali/tupassi-perche-la-sanzione-del-garante-privacy-e-un-monito-per-gli-sviluppatori...

TuPassi: perché la sanzione del Garante privacy è un monito per gli sviluppatori software Home Norme e adeguamenti Privacy e Dati personali La sanzione comminata dal Garante privacy all'app TuPassi deve servire da monito a tutti gli sviluppatori software e far comprendere che, per essere competitivi ed evitare di vanificare gli investimenti effettuati, occorre tenere in debita considerazione i profili connessi alla protezione dei dati personali. Ecco perché 1 minuto fa S Nicola Sandon Associate, Tonucci & Partners V Alessandro Vasta Partner, Tonucci & Partners La mancata integrazione dei principi previsti dalla normativa privacy nei processi di sviluppo di un software può costare cara a tutti i soggetti coinvolti nella filiera, sia in termini economici che di reputazione: è questa la principale lezione che si può trarre dalla vicenda legata al sistema di prenotazione on-line TuPassi, oggetto nel corso degli ultimi dodici mesi di ben quattro provvedimenti del Garante per la Protezione dei Dati e di sanzioni amministrative per un valore complessivo di 540.000 euro. Indice degli argomenti App TuPassi: come funziona il sistema L'intervento del Garante I dettagli della sanzione all'app TuPassi Ecco perché la sanzione è monito per tutti gli sviluppatori Le misure correttive per lo sviluppatore Conclusioni App TuPassi: come funziona il sistema TuPassi è un sistema interattivo di gestione delle prenotazioni che consente agli utenti di prenotare servizi di sportello o fissare appuntamenti presso enti pubblici e soggetti privati. Il sistema, sviluppato da una società di Crema, risponde a delle esigenze ben precise: da un lato consente di snellire il processo di prenotazione, organizzando in maniera più efficiente e razionale i tempi e le risorse di aziende, professionisti ed enti pubblici, e dall'altro ha il pregio di evitare agli utenti lunghe e noiose code. I benefici sono concreti e mutuali. Gli utenti hanno a disposizione un ampio ventaglio di canali di cui usufruire per completare la propria prenotazione: esistono un'app e un sito dedicati, dei totem posizionati direttamente presso i locali dei soggetti che erogano le prestazioni prenotabili e in alcuni casi il servizio è (o meglio, era) disponibile presso altri soggetti che fungono da intermediari, quali le tabaccherie. Il funzionamento è quasi elementare: ci si registra sulla piattaforma del sistema di prenotazione, si seleziona il servizio e TuPassi fornisce la data e l'ora dell'appuntamento, che vengono anche confermate via e-mail. L'idea è innovativa, il sistema convince, domanda e offerta si incontrano e TuPassi inizia a essere impiegato da centinaia di

clienti sul territorio nazionale. L'intervento del Garante I guai iniziano nel 2018 quando il Nucleo Speciale Privacy della Guardia di Finanza sottopone ad un attento scrutinio il sistema di prenotazione nell'ambito di una verifica posta in essere presso l'ente territoriale "Roma Capitale", che faceva ampio uso della piattaforma TuPassi, impiegata in tutti i Municipi del Comune di Roma. Il Garante, al termine di una complessa istruttoria, individua con apposito provvedimento prescrittivo pubblicato nel marzo del 2019 svariate criticità legate all'impiego del sistema di prenotazione da parte dell'ente dal punto di vista della protezione dei dati personali, sia sotto il profilo tecnico che organizzativo, spesso riferibili alla struttura ed al funzionamento stesso della piattaforma TuPassi, quali: l'assenza di idonea informativa a utenti e dipendenti dei trattamenti effettuati per mezzo del sistema ai sensi dell'art. 13 del GDPR; la particolare funzionalità di reportistica connessa alla piattaforma, in grado di operare un controllo a distanza sui dipendenti, ricadendo pertanto nell'ambito di applicazione dell'art. 4 della L. 300/1970; la mancata nomina del fornitore del sistema a responsabile del trattamento in relazione alle attività di assistenza e manutenzione del sistema; la non adeguatezza delle misure di sicurezza adottate, con particolare riferimento all'utilizzo del protocollo http per il traffico tra i server di e i totem impiegati negli uffici dell'ente; l'impossibilità di configurare caso per caso la tipologia dei dati ed i tempi massimi di conservazione nel sistema. Le carenze rilevate risultano idonee a causare la violazione della vigente normativa, rendendo illecito il trattamento dei dati di utenti e dipendenti posto in essere dall'ente capitolino mediante il sistema di prenotazione: il Garante, dunque, si congeda imponendo sia a "Roma Capitale", nella sua qualità di titolare del trattamento, che allo sviluppatore lombardo, qualificato come responsabile del trattamento ai sensi dell'art. 28 del GDPR, una serie di misure correttive e avvertendo che un autonomo procedimento sanzionatorio è già stato avviato. I dettagli della sanzione all'app TuPassi Procedimento sanzionatorio che giunge a termine nel dicembre del 2020, con l'emissione di tre diversi provvedimenti, due dei quali rivolti espressamente a Miropass S.r.l., la società che ha progettato TuPassi e lo fornisce all'ente con regolare contratto di licenza. In particolare, "Roma Capitale" viene sanzionata per 500.000 euro a causa dell'illiceità dei trattamenti posti in essere anteriormente agli accertamenti che hanno portato all'emissione del primo provvedimento, mentre lo sviluppatore non solo si vede elevare a sua volta una sanzione di 40.000 euro per la medesima ragione, ma diviene anche destinatario di un provvedimento ingiuntivo che gli intima di: procedere entro 30 giorni alla trasmissione dello stesso a tutti i "soggetti pubblici e privati che attualmente utilizzano il sistema "TuPassi" con le modalità di impiego e le criticità già accertate dal Garante" con il primo provvedimento del marzo 2019; avviare i necessari aggiornamenti al sistema per assicurare la piena conformità dei trattamenti alla disciplina vigente in materia di protezione dei dati. Ecco perché la sanzione è monito per tutti gli sviluppatori DIRETTA LIVE, 24 FEBBRAIO A confronto con i Security People: come realizzare un piano di sicurezza davvero efficace? Sicurezza Cybersecurity Cosa aspetti? Iscriviti subito! La vicenda in esame appare degna di nota soprattutto per quanto

riguarda l'attenzione dedicata dal Garante allo sviluppatore/fornitore del sistema di prenotazione: infatti, al di là delle condotte illecite poste in essere dai soggetti coinvolti nel trattamento (variegate e senz'altro rilevanti, ma sulle quali non ci soffermeremo), è innegabile che particolare rilievo tra i profili di criticità rilevati dall'Autorità abbiano assunto le carenze mostrate by design "dalle specifiche caratteristiche del sistema" di prenotazione TuPassi. Carenze che, in alcune ipotesi, sono state di per sé sole sufficienti a determinare la non conformità dei trattamenti posti in essere. Le misure correttive per lo sviluppatore Un primo elemento di interesse è senz'altro rappresentato dalla decisione del Garante di intervenire direttamente nei confronti dello sviluppatore della piattaforma - destinatario di specifiche misure correttive sin dal primo provvedimento del 2019 e poi di separato provvedimento sanzionatorio nel 2020 -, sfruttando un'interpretazione estensiva dei principi di privacy by design e by default di cui all'art. 25 del GDPR[1]. L'Autorità, infatti, se da un lato ha espressamente riconosciuto che il tenore letterale della norma sarebbe tale da escludere i responsabili del trattamento dalla diretta applicabilità dei suddetti principi, dall'altro ricorda che il considerando 78 al Regolamento si rivolge espressamente agli sviluppatori "di prodotti, servizi e applicazioni", invitandoli a "tenere conto del diritto alla protezione di dati sin dalla fase della progettazione" ed "a far sì che i propri clienti possano adempiere ai propri obblighi" in materia di privacy, imponendo a Miropass S.r.l. di mettere in atto le "misure tecniche e organizzative adeguate richieste dallo stesso art. 25 del Regolamento". Il precedente è di assoluto rilievo: ove il Garante rilevi, anche incidentalmente, che un software, una piattaforma o una soluzione tecnologica non è in grado, per elementi insiti nella sua progettazione, di consentire al titolare del trattamento di rispettare i principi applicabili al trattamento dei dati, lo sviluppatore/produttore della stessa potrebbe essere direttamente chiamato dall'Autorità a rispondere di tali difetti e/o a porvi, a prescindere dall'utilizzo che ne faccia il licenziatario. È poi opportuno richiamare l'attenzione sulla scelta del Garante di imporre a Miropass S.r.l. di allertare tutti i propri clienti che facciano uso della piattaforma TuPassi delle carenze individuate dall'Autorità e della potenziale illiceità dei trattamenti posti in essere sulla base della stessa. La scelta di una simile misura appare perfettamente in linea con il fatto che parte dei rilievi formulati nei confronti di "Roma Capitale" si basino su carenze intrinseche del sistema di prenotazione, in quanto tali idonee a ricorrere a prescindere dall'utilizzatore. Com'è facile intuire, il potenziale impatto di un simile provvedimento sulla reputazione di una società il cui core business è la fornitura del sistema stesso è estremamente elevato ed in grado danneggiare in maniera concreta e persistente il fatturato dell'attività. Infine, è utile rammentare come i rilievi del Garante siano concretamente idonei ad aprire la strada a domande civili di risarcimento del danno nei confronti dello sviluppatore che fornisca un prodotto che presenti by design delle carenze dal punto di vista privacy da parte di tutti quei clienti ("Roma Capitale" in primis) che dovessero essere sanzionati a causa dell'accertata illiceità dei trattamenti di dati personali posti in essere per mezzo del software TuPassi.

Conclusioni Nel mondo dell'industria 4.0, della digitalizzazione e della connettività, rivolgersi a fornitori terzi specializzati per la soluzione di problemi di efficienza e razionalizzazione dei processi mediante l'impiego di soluzioni tecnologiche innovative è una prassi consolidata, in grado di portare rilevanti benefici a tutti i soggetti coinvolti. Non bisogna però dimenticare che l'impiego di tali soluzioni spesso e volentieri si accompagna necessariamente alla raccolta, analisi e conservazione di volumi di dati personali sempre più rilevanti, dando origine a rilevanti rischi per i diritti e le libertà delle persone fisiche, quali discriminazione, esclusione sociale, sorveglianza di massa, e che, ove tali trattamenti non si svolgano nel rispetto della vigente normativa, i rischi cui ci si espone sono molteplici, e spesso possono essere ben più gravi delle semplici sanzioni economiche. Si pensi ad una società di retail B2C che crea nel tempo un'enorme banca dati dei propri clienti per finalità di marketing che si trova nell'impossibilità di utilizzarla o cederla a terzi perché il software impiegato per la raccolta del consenso non è conforme alle disposizioni del GDPR. O ancora ad un ente pubblico o privato (es. call center) che investe tempo e denaro nella strutturazione di un processo di valutazione delle performance dei dipendenti basato su un apposito applicativo per poi vedersi ordinare dalle autorità la dismissione dello stesso per violazione delle norme in materia di controllo a distanza dei lavoratori. È dunque necessario che gli stakeholders comprendano che, per essere sempre più competitivi ed evitare di vanificare gli investimenti effettuati sarà sempre più irrinunciabile tenere in debita considerazione i profili connessi alla protezione dei dati personali, integrando efficacemente i principi previsti dalla normativa privacy - ed in particolar modo quelli connessi alla privacy by design e by default - sin dalle prime fasi di sviluppo e progettazione di tali soluzioni tecnologiche. La vicenda legata all'applicativo TuPassi fornisce un ottimo esempio di come un intervento tardivo in tale ambito possa seriamente danneggiare lo sviluppatore e i propri clienti, sia sotto un profilo economico che reputazionale. NOTE "1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. 2.Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche

senza l'intervento della persona fisica. [ ]". WHITEPAPER Come vendere un maggior numero di soluzioni di data protection? Sicurezza dei dati Scarica il Whitepaper