Informazioni sulla PIA

Nome della PIA
Pin Bike Srl

Nome autore
Avv. Nicola Gargano – P.I. Graziano Albanese

Nome valutatore
Graziano Albanese

Nome validatore
Nicola Gargano

Data di creazione
12/07/2018

Nome del DPO/RPD

Parere del Valutatore e del Validatore
Le finalità di trattamento e le modalità di trattamento rispettano la base giuridica forte del titolare, che riceve consenso informato per il trattamento dei dati. Il trattamento, riguarda la raccolta di dati anagrafici, e dei dati relativi alla geolocalizzazione degli interessati, raccolti nello spostamento degli stessi nel percorso svolto per recarsi dalla loro abitazione al luogo di lavoro. I dati di geolocalizzazione sono resi disponibili dagli interessati con facoltà di scelta legata all'attivazione manuale del dispositivo di raccolta della posizione GPS, con l'interazione della APP resa loro disponibile per dispositivi Android e iOS. Gli interessati possono decidere quanto condividere la loro posizione. La raccolta della posizione degli interessati è finalizzata al raggiungimento di obiettivi. Gli interessati al raggiungimento di obiettivi legati ai km percorsi, ricevono un punteggio che può essere convertito in benefit, che consistono in acquisti di beni di consumo in negozi convenzionati o, la possibilità di ricevere sgravi fiscali concessi dai Comuni, che hanno sottoscritto un contratto d'uso della piattaforma per migliorare e promuovere la mobilità sostenibile nei centri urbani anche per i percorsi casa-lavoro. Inoltre tramite l'uso della APP disponibile per i device mobili, gli interessati a seguito di consenso informato raccolto in fase di adesione e di sottoscrizione del servizio, potranno ricevere informazioni e offerte commerciali dei negozi e delle attività commerciali che hanno aderito al progetto, e per la città per il quale l'interessato ha formalizzato la sottoscrizione del servizio.

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
E' richiesto il parere del Garante italiano, trattandosi di raccolta di dati con geolocalizzazione mirata ad incrementare la mobilità sostenibile, in cambio di benefit fiscali e relativi ad acquisti di beni di consumo.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?
Il trattamento riguarda l'acquisizione di dati comuni di persone fisiche attraverso l'uso di una APP per dispositivi mobili e di un sito web.

Quali sono le responsabilità connesse al trattamento?
Il Titolare è responsabile della raccolta dei dati e della loro gestione fatta dagli incaricati, dell'archiviazione, e di tutte le fasi di gestione fino al loro trasferimento esterno previsto per il raggiungimento delle finalità ultime in capo al titolare ed all'interessato. Inoltre il Titolare è responsabile dei dati acquisiti tramite la fornitura dei servizi stessi, in quanto questi permettono di raccogliere tendenze ed abitudini degli interessati.

Ci sono standard applicabili al trattamento?
Per assolvere a tutti gli obblighi del trattamento il Titolare ha selezionato servizi e partner già GDPR compliance.
I dati raccolti vengono archiviati su piattaforma Amazon AWS, Irlanda.
Amazon.com è conforme al GDPR perché si è attenuta al codice di condotta CISPE e risulta già iscritta al Privacy Shield.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati trattati: dati comuni ed anagrafici
Dati relativi alla geolocalizzazione ed alla raccolta delle abitudini degli interessati, che riguardano i loro spostamenti con la possibilità di raccogliere in un prossimo futuro anche i dati relativi al loro spostamento casa-lavoro. I dati sono raccolti in forma anonima.

I dati sono raccolti in archivi elettronici (database) con la suddivisione dei dati anagrafici dai dati di profilazione delle tendenze dell'interessato, quindi pseudonimizzati.

I dati acquisiti, vengono cancellati su richiesta dell'interessato, o dopo 5 anni dall'ultimo trattamento utile. Per ultimo trattamento utili si intende se effettuato con l'invio di comunicazioni e con lo scambio o la raccolta di informazioni fatte sull'interessato e dall' interessato.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

1) acquisizione dei dati tramite sito web e app (dati comuni)

- acquisizione su database informatico
- accesso permesso solo agli incaricati
- backup automatico gestito dal provider

2) acquisizione di dati di profilazione geolocalizzata

- acquisizione automatica su database informatico
- dati raccolti in forma anonima con pseudonimizzazione
- backup automatico gestito dal provider

Quali sono le risorse di supporto ai dati?

Formato elettronico
Dati archiviati su Amazon.com su server in Europa
Amazon.com è conforme al GDPR perché si è attenuta al codice di condotta CISPE e risulta già iscritta al Privacy Shield.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I trattamenti si basano su un esplicito consenso raccolto dagli interessati. I dati acquisiti inoltre sono quelli minimi ed indispensabili per la fornitura dei servizi presentati ed accettati dagli interessati.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Base giuridica contrattuale raccolta anche con il consenso.

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Si

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati sono acquisiti direttamente dall'interessato, e pertanto ritenuti accurati, è cura dell'interessato mantenerli aggiornati per continuare a ricevere i servizi sottoscritti.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati sono acquisiti per un periodo di massimo 5 anni dopo l'ultimo trattamento effettuato, inoltre gli interessati godono del diritto di cancellazione che prevede per loro la possibilità di eliminare ogni dato acquisto che vada oltre i meri dati anagrafici.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Preventivamente alla raccolta dei dati viene sottoposta una informativa con tre distinte voci di consenso.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso viene acquisito mediante la tecnica del point and click su 3 distinte voci di consenso. Ci si propone di raccogliere il consenso relativamente ai minori di anni 14 mediante modulo sottoscritto con firma autografa da consegnarsi a mano o mezzo mail dal genitore o tutore legale del minore.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Tramite apposita modulistica resa disponibile sul sito www.pinbike.it
Il documento potrà essere inviato in diverse modalità, via posta ordinaria, posta elettronica o raccomandata o PEC.
Per praticità e stato preso in uso il modulo reso disponibile dal Garante per l'esercizio dei diritti degli interessati.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Tramite apposita modulistica resa disponibile sul sito www.pinbike.it
Il documento potrà essere inviato in diverse modalità, via posta ordinaria, posta elettronica o raccomandata o PEC.
Per praticità e stato preso in uso il modulo reso disponibile dal Garante per l'esercizio dei diritti degli interessati.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Tramite apposita modulistica resa disponibile sul sito www.pinbike.it
Il documento potrà essere inviato in diverse modalità, via posta ordinaria, posta elettronica o raccomandata o pec.
Per praticità e stato preso in uso il modulo reso disponibile dal Garante per l'esercizio dei diritti degli interessati.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Il Titolare ha provveduto a regolarizzare i rapporti con l'unica figura identificata come responsabile del trattamento mediante atto di nomina a responsabile del trattamento sottoscritta da ambo le parti.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati saranno trattati esclusivamente nel territorio dell'Unione Europea. Tuttavia, per ragioni tecniche e organizzative, i dati potranno essere trasferiti fuori dall'Unione Europea, presso **Amazon.com, Inc.** con sede in Seattle, Washington per cui già esiste una decisione di adeguatezza ai sensi del Capo V del Regolamento (UE) 2016/679 espressa dalla Commissione Europea attraverso il **Privacy Shield.** In ogni caso saranno comunicati solo i dati necessari per il perseguimento delle finalità di cui sopra.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

I dati vengono archiviati su Amazon AWS Irlanda e non sono crittografati.

Valutazione : Accettabile con impegno di verifica di implementazione della crittografia.

Anonimizzazione

I dati sono registrati in un unico database, il sistema di anonimizzazione è implementato grazie alla distribuzione dei dati su più tabelle presenti nello stesso.

Valutazione : Accettabile

Controllo degli accessi

Esiste una distinzione di accessi per funzionalità e tipi di dati da trattare.

Ogni incaricato dispone di credenziali di acceso agli archivi, per i quali è previsto periodicamente e con cadenza almeno semestrale il cambio della password.

Valutazione : Accettabile

Gestione postazioni

I Pc usati per il trattamento dei dati sono dotati di antivirus e firewall software aggiornato regolarmente.

Valutazione : Accettabile

Archiviazione

Periodicamente il titolare, provvede ad eseguire copia locale dei database archiviati sui server remoti.

Valutazione : Accettabile

Vulnerabilità

Le precauzioni volte a limitare le vulnerabilità relativi agli accessi abusivi o alla distruzione o trasferimento illecito dei dati, si basano sulle misure implementate da Amazon AWS. Tali misure sono idonee a garantire i livelli minimi di sicurezza, inoltre si prevede come ulteriore misure quella di avviare delle copie locali degli archivi.

Altro rischio relativo alle vulnerabilità, riguarda il rischio di perdita delle credenziali degli utenti che fanno accesso agli archivi, a seguito di frodi di phishing o furto delle credenziali. Per far fronte a questo tipo di rischio il Titolare ed il Responsabile, periodicamente aggiornano e fanno aggiornare le password delle credenziali di accesso agli incaricati.

Valutazione : Accettabile

Lotta contro il malware

I sistemi che fanno accesso ai dati sono tutti protetti con software antivirus e firewall regolarmente aggiornato.

Valutazione : Accettabile
Commento di valutazione :
E' previsto un piano periodico di verifica dell'implementazione delle misure minime di sicurezza informatica.

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

I dati acquisti non determinano particolari rischi degli interessati, trattandosi solo di dati anagrafici e di profilazione anonima su spostamenti.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Attacco informatico con perdita delle credenziali dei sistemi che accedono ai dati o alla piattaforma dove sono archiviati i dati, Blocco dei sistemi, Virus informatici, Perdita dei requisiti di sicurezza del provider.

Quali sono le fonti di rischio?

Errore umano, Virus informatici.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi, Archiviazione, Lotta contro il malware, Gestione postazioni.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata. Sarebbe utile implementare misure di crittografia dei dati. e che l'accesso e l'autenticazione ai dati possa avvenire su sistemi cloud tramite protocollo https.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Le provabilità e l'appetibilità dei dati sono bassi, per determinare un rischio importante per gli interessati.

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Perdita di dati anagrafici e delle abitudini di mobilità per raggiungere il luogo di lavoro.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Errore umano, Perdita delle credenziali, Virus informatico.

Quali sono le fonti di rischio?

Virus, Fonti umane interne ed esterne.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi, Gestione postazioni, Archiviazione, Lotta contro il malware.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata, Il rischio può ritenersi basso, è già implementato un piano di controllo periodico delle misure di sicurezza e delle procedure.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata. Le misure di sicurezza implementate, garantiscono un buon livello di sicurezza.

Valutazione : Accettabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita di dati anagrafici e delle abitudini di mobilità per raggiungere il luogo di lavoro.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Blocco dei sistemi, Errore umano, Virus informatico.

Quali sono le fonti di rischio?

Fonti umane interne ed esterne, Virus, Blocco fisico dei sistemi

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Archiviazione locale dei dati, su sistema esterno nella disponibilità del Titolare, dotato di crittografia.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, La perdita totale non comporta particolare rischio per gli interessati. Vanno però pianificate periodiche verifiche di integrità delle misure di sicurezza ed in particolare delle copie locali di backup.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Basso

Valutazione : Accettabile

Piano d'azione

Principi fondamentali

Pianificazione di azioni correttive e misure di controllo. Sistema del PDCA (Plan, do, check, act) sui sistemi di sicurezza informatica.

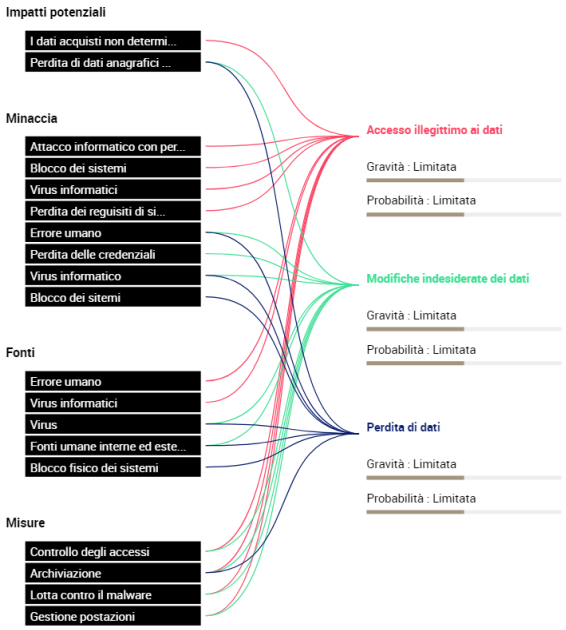
Misure esistenti o pianificate

E’ previsto un piano di verifica periodica delle misure di sicurezza informatica e della integrità delle copie di sicurezza dei dati archiviato in locale.

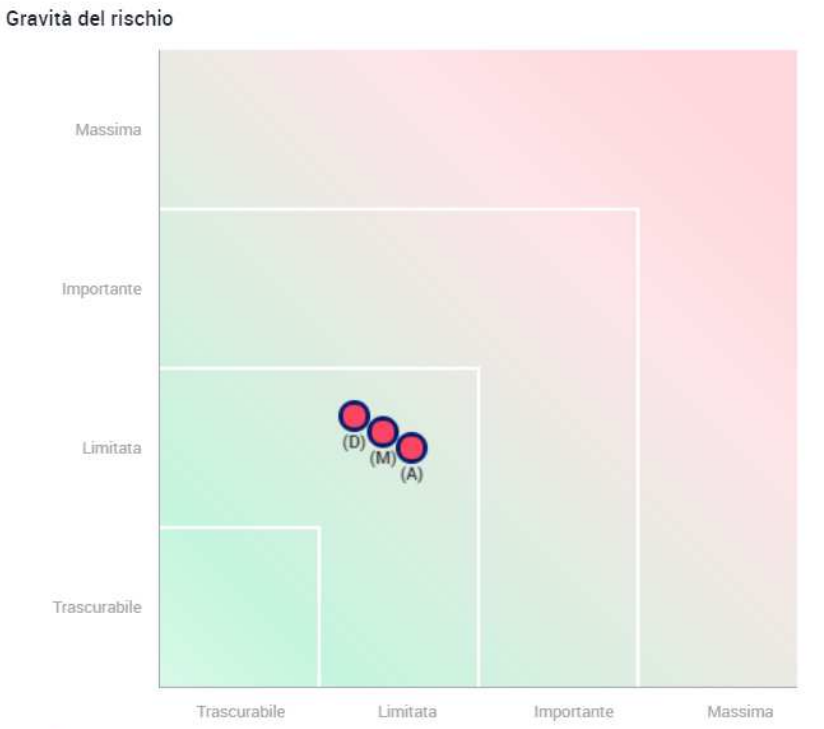
Rischi

E’ previsto un piano di verifica periodica delle misure di sicurezza informatica e della integrità delle copie di sicurezza dei dati archiviato in locale.

Panoramica dei rischi



Mappa dei rischi



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati