GDPR: le linee guida per i servizi di fornitura online

Queste linee guida sono molto interessanti perché si concentrano sulla base giuridica del trattamento ai sensi dell'articolo 6, paragrafo 1, **GDPR**.

Infatti, secondo l'*European Data Protection Board* (EDPB), identificare la base giuridica appropriata è di fondamentale importanza.

I titolari del trattamento devono tener conto dell'impatto sui diritti degli interessati e come questi cambiano in base all'identificazione della base giuridica.

L'articolo 6 GDPR, come detto, fornisce un decalogo di basi giuridiche del trattamento dei dati personali.

Il primo in disamina riguarda il **trattamento necessario per l'esecuzione di un contratto**: a volte gli obblighi contrattuali nei confronti dell'interessato non possono essere eseguiti senza che vengano trattati i dati personali dell'interessato.

Tale argomento viene sempre più in gioco nei servizi online in settori come i social media, l'e-commerce, ricerca, comunicazione e viaggi.

Questi servizi on line, specifica l'EDPB, sono:

- finanziati dai pagamenti degli utenti;oppure,
- sono forniti senza pagamento monetario da parte del consumatore e quindi sono finanziati dalla vendita dei servizi pubblicitari on line che consentono di prendere di mira i soggetti interessati e quindi i loro dati.

Il trattamento, osserva l'EDPB, spesso viene effettuato in modo tale che l'utente potrebbe non essere a conoscenza di come tale trattamento avvenga e su quale base giuridica, e rende quasi impossibile per l'interessato di esercitare qualsiasi controllo sull'uso dei propri dati.

In questo contesto, l'EDPB, ha ritenuto opportuno stilare delle indicazioni su quale base giuridica indicare e fornire all'interessato l'informazione del trattamento dei suoi dati.

Già il WP29 ha precedentemente espresso opinioni sulla base giuridica per finalità contrattuale.

Questo tipo di base giuridica, tuttavia, osserva l'EDPB deve essere marginale e non esteso a tutti i tipi di trattamento che derivano dai servizi on line.

Le linee guida qui in commento, osservano che il trattamento è lecito a mente dell'articolo 6, paragrafo 1, lettera b), del GDPR, solo quando il trattamento risulti strettamente "necessario per l'esecuzione di un contratto".

Inoltre, i servizi erogati online coinvolgono anche altri tipi di regolamentazione quali la tutela dei consumatori e della concorrenza.

Pertanto, lo stesso EDPB, tiene a precisare che le considerazioni delle linee guida possono essere di ausilio anche in altri settori, oltre lo scopo precipuo del trattamento dei dati personali.

L'EDPB, infatti, osserva che i contratti e le condizioni contrattuali debbano essere conformi ai requisiti delle leggi sui contratti e, a seconda dei casi, conforme a previsioni e tutele specifiche quali ad esempio nei contratti dei consumatori (si pensi al quadro normativo delle clausole abusive).

Quindi, l'EDPB dichiara che i titolari dovrebbero sempre

assicurarsi di rispettare i principi di protezione dei dati di cui all'articolo 5 e tutti gli altri requisiti del GDPR e, se del caso, della legislazione *ePrivacy*.

Ciò significa che il trattamento dei dati personali sia effettuato in modo equo e trasparente e in linea con la limitazione delle finalità e obblighi di minimizzazione dei dati.

Invero l'articolo 5, paragrafo 1, lettera a), del GDPR prevede che i dati personali siano trattati in modo **lecito**, **equo** e **trasparente** in relazione al profilo dell'interessato.

L'EDPB chiarisce il significato di questo precetto.

- Il principio di equità include il riconoscimento delle ragionevoli aspettative delle persone interessate, in considerazione delle possibili conseguenze negative del trattamento dei dati su di loro, e avendo riguardo alla relazione e ai potenziali effetti dello squilibrio tra loro e i titolari.
- Per legalità si intende quel requisito di validità che, ai sensi del diritto contrattuale applicabile, i servizi on line dovrebbero avere.

Un esempio di invalidità riguarda l'ipotesi che l'interessato sia un minore, che come noto, nel nostro ordinamento non ha capacità di agire.

- L'articolo 5 (1) (b) del GDPR prevede il principio di limitazione delle finalità, che impone che i dati vengano raccolti solo per scopi **specifici, espliciti e legittimi** e non ulteriormente trattati in modo da straripare con tali scopi.

Inoltre lo stesso articolo 5, paragrafo 1, lettera c), prevede la minimizzazione del dato e cioè il trattamento di un numero di dati il più ridotto possibile.

In precedenza il WP29 ha precedentemente dichiarato che lo scopo della raccolta deve essere chiaramente e specificamente identificato: deve essere dettagliato abbastanza da determinare quale tipo di trattamento sia o no incluso nello scopo specificato e per consentire di valutare la conformità alla legge e salvaguardare la protezione dei dati.

Per questo motivo, continua il WP29, uno scopo vago o generico, come ad esempio "migliorare" l'esperienza degli utenti, "scopi di marketing", "scopi di sicurezza IT", senza alcun ulteriore dettaglio, non soddisfa i criteri di specificità

Base giuridica contrattuale (articolo 6, par.1, lett.b) e altre basi giuridiche.

L'EDPB chiarisce che quando il trattamento non è considerato "necessario per l'esecuzione di un contratto", ovvero quando il servizio richiesto può essere fornito senza che vengano trattati i dati, può essere applicabile un'altra base giuridica a condizione che siano soddisfatte le condizioni specificamente previste.

- In particolare, in alcune circostanze può essere più appropriato ottenere il consenso liberamente concesso ai sensi dell'articolo 6, paragrafo 1, lettera a).
- Oppure sarebbe appropriata un base giuridica a mente delle lettere b) ed f) dello stesso articolo.

In ogni caso ed obbligatoriamente **le basi giuridiche devono essere identificate prima ed all'inizio del trattamento e le informazioni fornite agli interessati devono essere fornite a mente degli artt. 13 e 14 GDPR**.

Inoltre, precisa l'EDPB, che laddove il trattamento non abbia come base giuridica la necessaria esecuzione di un contratto,

tale trattamento può aver luogo solo se si sia preventivamente stabilita un'altra base giuridica, appropriata al trattamento dati specifico.

In linea con i **l'obbligo di trasparenza**, i titolari del trattamento dovrebbero evitare qualsiasi confusione in merito a qual base giuridica sia applicabile.

Infatti, a seconda dei casi, le persone interessate potrebbero erroneamente avere l'impressione di dare il loro consenso a mente dell'articolo 6, paragrafo 1, lettera a), GDPR, al momento della firma di un contratto o dell'accettazione di termini di servizio.

Allo stesso modo, il titolare potrebbe erroneamente presumere che la firma di un contratto corrisponda ad un consenso valido come base giuridica.

È importante, quindi, sempre distinguere tra stipulare un contratto e fornire un consenso valido per il trattamento dei dati.

Applicazione pratica della base giuridica dell'articolo 6, paragrafo 1, lettera b), GDPR.

Anzitutto, l'EDPB ribadisce che l'articolo 6, paragrafo 1, lettera b), GDPR, si applica se il trattamento sia obiettivamente necessario per l'esecuzione di un contratto con un interessato, ovvero anche per situazioni precontrattuali.

Quindi è necessario

(a) che vi sia un contratto,

(b) che il contratto sia valido ai sensi delle leggi contrattuali nazionali applicabili; e

(c) che il trattamento sia oggettivamente necessario per l'esecuzione del contratto, in caso negativo dovrebbe essere il titolare considerare un'altra base giuridica per il

trattamento.

Il concetto di “necessità”

La necessità del trattamento come indicato nell’articolo 6, paragrafo 1, lettera b) è un prerequisito sia per i titolari che per gli interessati.

Valutare ciò che è “necessario” implica una valutazione combinata dello scopo perseguito dal titolare e la capacità invasiva del trattamento nei riguardi dell’interessato.

Se esistono quindi alternative al trattamento meno invasive significa che il trattamento dei dati non è “necessario” per l’esecuzione del contratto.

I contratti per i servizi digitali possono includere termini espressi che impongono condizioni aggiuntive pubblicità, pagamenti o cookies, etc..

Un contratto non può allargare artificiosamente le categorie di dati personali o tipi di trattamento per fondare la base giuridica ai sensi dell’articolo 6, paragrafo 1, lettera b).

L’EDPB fornisce una check list di domande per valutare se l’articolo 6, paragrafo 1, lettera b) sia applicabile oppure no.

Eccole:

- Qual è la natura del servizio fornito all’interessato?
- Quali sono le caratteristiche distintive?
- Qual è l’esatta logica del contratto (cioè la sua sostanza e l’oggetto fondamentale o come diremmo in Italia, la “causa” del contratto)?
- Quali sono gli elementi essenziali del contratto?
- Quali sono le prospettive e le aspettative reciproche delle parti del contratto?
- Come è stato promosso o pubblicizzato il servizio

all’interessato?
- Un utente normale ragionevolmente abbia compreso che, considerando la natura del servizio, il trattamento avverrà solo per eseguire il contratto?

Se all’esito di queste domande la valutazione sul trattamento sia quella di renderlo necessario per l’esecuzione di un contratto allora si potrà invocare come base legittima quella dell’art. 6, par.1, lett. b, GDPR.

Vediamo gli esempi forniti dall’EDPB

Esempio 1

Una persona interessata acquista articoli da un rivenditore on-line.

L’interessato desidera pagare con carta di credito per i prodotti da consegnare a casa.

Per soddisfare il contratto, il rivenditore deve elaborare i dati della carta di credito del soggetto e l’indirizzo di fatturazione a scopo di pagamento e l’indirizzo dell’interessato per la consegna. Pertanto, l’articolo 6, paragrafo 1, lettera b) è applicabile come base giuridica per queste attività di trattamento.

Tuttavia, se il cliente ha optato per la spedizione a un punto di raccolta, il trattamento dei dati dell’indirizzo di casa del soggetto non è più necessario per l’esecuzione del contratto di acquisto e quindi si avrà una diversa base giuridica rispetto all’articolo 6, paragrafo 1, lettera b).

Esempio 2

Lo stesso rivenditore on-line desidera creare profili sui gusti e sulle scelte di vita dell'utente in base a sue visite al sito web.

L'esecuzione del contratto di acquisto non dipende dalla profilazione.

Anche se la profilazione è specificamente menzionata nel contratto, ciò solo non rende "necessario" il trattamento per l'esecuzione del contratto.

Se il rivenditore on-line desidera effettuare tale profilazione, ha bisogno di fare affidamento su una base giuridica diversa.

Servizi aggregati

I titolari del trattamento sono liberi di programmare e progettare i loro affari, servizi e contratti.

In alcuni casi, un titolare potrebbe raggrupparne diversi servizi con diverse caratteristiche in un unico contratto.

Ciò potrebbe creare una situazione, come afferma l'EDPB, "prendi o lascia" per gli interessati che potrebbero essere interessati ad uno solo dei servizi.

Laddove il contratto sia costituito da diversi servizi separati o separabili l'uno dall'altro, si pone la questione se ed in che misura l'articolo 6, paragrafo 1, lettera b) possa fungere da base giuridica.

In generale l'EDPB nega la validità della base giuridica sul presupposto della necessaria esecuzione del contratto poiché il trattamento non si rende necessario per i singoli servizi richiesti dall'interessato, ma piuttosto per il modello di business più ampio del voluto dal titolare.

Risoluzione del contratto

Come detto, il titolare deve identificare la base giuridica appropriata per ogni tipo di trattamento previsto prima che il trattamento stesso avvenga.

Ciò dovrebbe riguardare anche il caso della risoluzione del contratto dove il trattamento dei dati non sarà più necessario per l'esecuzione di un contratto (ormai risolto) e quindi il titolare non potrà più trattare i dati.

Quindi dovrebbe cambiare la base giuridica del trattamento rispetto a quella originaria.

Ad esempio quando l'interessato presti il proprio consenso al trattamento dopo la risoluzione (la base giuridica nuova sarà il consenso).

L'articolo 17, paragrafo 1, lettera a), GDPR prevede che i dati personali siano cancellati quando non sono più necessari in relazione agli scopi per cui sono stati raccolti.

Tuttavia, tale precetto non si applica se il trattamento è necessario per determinati scopi specifici, quali l'esercizio del diritto di difesa a mente dello stesso articolo.

Ciò che sarà importante per i titolari che vorranno fare affidamento a basi giuridiche diverse è quello di identificare le corrette basi giuridiche all'inizio del trattamento e comunicarle preventivamente all'interessato.

Esempio 3

Un servizio online offre un servizio di abbonamento che può essere annullato in qualsiasi momento. Quindi, il titolare del trattamento fornisce informazioni all'interessato sul trattamento dei dati personali.

Il titolare del trattamento spiega che finché il contratto è

in vigore, tratterà i dati relativi a utilizzo del servizio per emettere fatture.

La base giuridica è l'articolo 6, paragrafo 1, lettera b), come trattamento per gli scopi di fatturazione necessari per l'esecuzione del contratto.

Tuttavia, quando il contratto viene risolto e presupponendo che non vi sia alcuna necessità di conservare i dati per scopi difensivi, la cronologia sui dati verrà eliminata.

Inoltre, il titolare del trattamento dovrà informare gli interessati che ha un obbligo di trattenere

alcuni dati personali a fini contabili per un numero specificato di anni (in Italia 10 anni).

La base giuridica in questo caso sarà quella descritta dall'articolo 6, paragrafo 1, lettera c), e la conservazione avverrà anche in caso di risoluzione del contratto.

Base giuridica prima della stipula di un contratto

La base giuridica dell'articolo 6, paragrafo 1, lettera b), GDPR può essere utilizzata prima che venga stipulato un contratto al fine di facilitare l'effettiva stipulazione del contratto stesso.

Tale assunto non riguarda ovviamente i servizi di marketing.

Esempio 4

Una persona interessata fornisce il proprio codice postale per verificare se un determinato fornitore di servizi opera nella propria area.

Questo può essere considerato come un trattamento necessario

per facilitare l’eventuale stipula di un probabile contratto.

Esempio 5

In alcuni casi, gli istituti finanziari hanno il dovere di identificare i loro clienti in base alla normativa nazionale.

Quindi, prima di stipulare un contratto con gli interessati, una banca richiede di esaminare un documento di identità.

In questo caso, l’identificazione è necessaria per un obbligo giuridico in capo alla banca piuttosto che per prendere fornire il servizio all’interessato.

Pertanto, la base giuridica appropriata non è l’articolo 6, paragrafo 1, lettera b), ma l’articolo 6, paragrafo 1, lettera c).

Trattamento per il “miglioramento del servizio”

I servizi online raccolgono spesso informazioni dettagliate su come gli utenti interagiscono con il loro servizio.

Nella maggior parte dei casi, la raccolta di tali dati non possono essere considerati necessari per la fornitura del servizio in quanto il servizio potrebbe essere erogato anche assenza di questo tipo di trattamento.

Tuttavia, il titolare potrebbe ricorrere ad altri basi giuridiche come l’interesse legittimo o il consenso.

L’EDPB non ritiene che l’articolo 6, paragrafo 1, lettera b) possa essere una base giuridica appropriata per il trattamento dei dati ai fini del miglioramento di un servizio o dello sviluppo di nuove funzioni del servizio stesso.

Nella maggior parte dei casi, un utente stipula un contratto

per avvalersi di un servizio esistente. Mentre la possibilità di miglioramenti e modifiche esula dall'esecuzione del contratto stesso.

Trattamento per la "prevenzione delle frodi"

Il trattamento ai fini preventivi di frodi può comportare monitoraggio ed una profilazione clienti (quindi interessati).

Secondo l'EDPB, è probabile che tale trattamento esuli da quanto oggettivamente necessario per l'esecuzione di un contratto con un interessato.

Tale trattamento, ancorché lecito, dovrà fare affidamento su un'altra base giuridica prevista dall'articolo 6, come ad esempio obblighi legali o interessi legittimi.

Trattamento per pubblicità comportamentale online

Viene spesso utilizzata la pubblicità comportamentale online ed il tracciamento di profili associati agli interessati.

Come regola generale, la pubblicità comportamentale non ha come base giuridica l'articolo 6 cit. non essendo elemento necessario dei servizi online.

Normalmente, sarebbe difficile sostenere che il contratto non è stato eseguito perché non c'erano annunci comportamentali.

Inoltre gli interessati hanno il diritto assoluto ai sensi dell'articolo 21 GDPR, di opporsi al trattamento dei loro dati a fini di commercializzazione diretta.

Inoltre l'EDPB afferma che i dati personali non possono essere considerati come merce scambiabile.

Le persone interessate possono accettare il trattamento dei propri dati personali, ma non possono commerciare i loro diritti fondamentali.

Infatti al punto 51 (vedi anche nota 28) delle linee guida l'EDPB afferma che i"*personal data cannot be considered as a tradeable commodity. Data subjects can agree to processing of their personal data, but cannot trade away their fundamental rights*".

L'EDPB rileva come, ad esempio per i cookies, i titolari debbano ottenere il consenso preventivo degli interessati per fare uso dei cookies nella pubblicità comportamentale.

L'EDPB osserva inoltre che il tracciamento e la profilazione degli utenti possono essere effettuati allo scopo di identificare gruppi di individui con caratteristiche simili, per consentire di indirizzare la pubblicità ad pubblico un pubblico più vasto.

Tale trattamento non può essere effettuato sulla base dell'articolo 6, paragrafo 1, lettera b), in quanto non si può dire essere obiettivamente necessario per l'esecuzione del contratto che l'interessato venga tracciato, profilato o confrontato con altri interessati per scopi pubblicitari.

Trattamento per la personalizzazione del contenuto

L'EDPB riconosce che la personalizzazione dei contenuti può (ma non sempre) costituire un elemento essenziale per alcuni servizi online e pertanto può essere considerato necessario per l'esecuzione del contratto.

Tale requisito dipende dalla natura del servizio fornito e non può essere eluso a vantaggio dei titolari del trattamento.

Ad esempio, il denaro è numerabile, il che significa che i

prezzi possono essere comparati in un mercato concorrenziale e i pagamenti monetari possono normalmente essere effettuati solo con i soggetti interessati coinvolti.

Viceversa, un servizio può essere promosso agli utenti senza personalizzazione.

Dove cioè la personalizzazione dei contenuti non è oggettivamente necessaria ai fini del contratto sottostante.

In questo caso deve essere prevista e considerata una base giuridica alternativa, ove applicabile.

Esempio 6

Un sito di notizie online offre agli utenti un servizio di aggregazione di notizie.

Il servizio scelto dall'utente consiste nel fornire agli utenti contenuti su misura da più fonti online attraverso un'unica interfaccia (una rassegna stampa).

Per fare questo, chiede agli utenti di creare un profilo sui loro interessi.

In questo caso, la personalizzazione ai fini della consegna dei contenuti può essere considerata obiettivamente necessaria per l'esecuzione del contratto tra l'azienda e l'utente, perché l'erogazione del servizio riguarda direttamente il contenuto personalizzato (quindi l'articolo 6 (1) (b) può essere una valida base giuridica applicabile).

Esempio 7

Un motore di ricerca di hotel online monitora le precedenti prenotazioni degli utenti per creare un profilo sulle loro spese.

Questo profilo viene successivamente utilizzato per

raccomandare particolari hotel all’utente quando deve fornire i risultati della ricerca da parte dell’interessato.

In questo caso, la profilazione del comportamento passato dell’utente e dei dati finanziari non sarebbe obiettivamente necessario per l’esecuzione di un contratto, ovvero la fornitura di servizi di ospitalità basati su particolari criteri di ricerca forniti dall’utente.

Pertanto, l’articolo 6, paragrafo 1, lettera b) non sarebbe applicabile a questa attività di trattamento.

Esempio 8

Un mercato online consente ai potenziali acquirenti di cercare e acquistare prodotti. Il mercato

desidera proporre suggerimenti di prodotti personalizzati in base agli elenchi dei potenziali acquirenti precedentemente visualizzati sulla piattaforma per aumentare l’interattività.

Questa personalizzazione non è oggettivamente necessaria per fornire il servizio reso dalla piattaforma di mercato.

Pertanto, tale trattamento di dati personali non può basarsi sull’articolo 6, paragrafo 1, lettera b) come base giuridica.

https://www.key4biz.it/gdpr-linee-guida-servizi-fornitura-online/256555/

Xinjiang Surveillance App

Targets Legal, Everyday Behaviour: Rights Group

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/WUQU48B8CPc/xinjiang-surveillance-app-targets-legal-everyday-behaviour-rights-group

---

Alphabet, pesano le multe a Google. Male utili e pubblicità

Dopo **Facebook** e **Amazon**, tocca alla holding di **Google** dichiarare i dati dei primi mesi del 2019 al resto del mondo. **Alphabet** però, ha deluso le aspettative degli analisti, con risultati superiori a quelli dello scorso esercizio, ma non in linea con le attese.

Nonostante un anno pieno di turbolenze interne, tra problemi legati alla privacy e multe internazionali comminate per violazione delle norme antitrust, i ricavi si sono attestati a 36,3 miliardi di dollari, in aumento del 17% sull'anno precedente, ma al di sotto delle stime degli analisti che avevano indicato una quota superiore ai 37 miliardi.

8,2 miliardi di multe Ue

L'utile netto che si attesta a 6,7 miliardi con una flessione del 29%, anche a causa della maximulta decisa dalla **Commissione europea** a marzo per abuso di posizione dominante.

L’ultima multa in ordine di arrivo risale a marzo 2019, quando la Commissione Europea capitanata dal Commissario sceriffo **Margrethe Vestager** impose a Google il pagamento di 1,49 miliardi di euro per violazione delle norme **antitrust dell’Ue.** Questa multa se sommata all’altra multa di luglio scorso di 4,43 miliardi per il ‘Caso Android’ più i 2,2 miliardi di giugno 2017 per abuso di posizione dominante nel campo dei motori di ricerca, l’ammontare complessivo arriva a 8,2 miliardi di euro di multe accumulate nel giro di due anni.

In termini di utili per azione, si è passati a 9,5 dollari dai 13,33 di inizio 2018; al netto dell’ ultima multa il dato è stato di 11,90 dollari, sopra le attese degli analisti per 10,61 dollari.

Amazon vero competitor dell’advertising

Il business pubblicitario di Alphabet resta ancora la punta di diamante, ma se da un lato la crescita ha contribuito ad aumentare le entrate complessive del 17%, ciò è stato inferiore a quello che gli investitori si aspettavano.

Perché sebbene il 92% delle ricerche Web avvenga sul motore di ricerca numero uno al mondo, oltre la metà delle persone che acquistano un prodotto online ormai si affidano oggi ad **Amazon**, aumentando il proprio business pubblicitario.

Pubblicità in perdita

I ricavi generati dalla pubblicità sono stati di 30,7 miliardi, in aumento di solo il 15% rispetto a un anno prima e al di sotto della media del 21% dei precedenti otto trimestri. Il gruppo ha dato la colpa a “variazioni significative” nei

tassi di cambio e alla “tempistica di cambiamenti dei prodotti pubblicitari”.

Il numero di click fatti dagli internauti su pubblicità apparse su siti legati a Google (il motore di ricerca, Gmail, YouTube) e che hanno generato introiti sono saliti del 39% annuo ma scesi del 9% rispetto all’ultimo trimestre del 2018. Il cost-per-click (una misura dei prezzi per la pubblicità attentamente monitorata) e’ pero’ calato del 19% annuo mentre e’ salito del 5% trimestre su trimestre. Nel trimestre le “impression” (quanto spesso una pubblicità e’ vista sulle proprietà dei partner di Google) sono aumentate del 6% annuo e il “cost-per-impression” (quanto Google puo’ fare pagare per quelle visioni) e’ salito dell’1%.

https://www.key4biz.it/alphabet-pesano-le-multe-a-google-male-utili-e-pubblicita/256254/

Apple Claims Parental Control Apps Removed Due to Use of MDM

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Q5yblJGQULU/apple-claims-parental-control-apps-removed-due-use-mdm

---

Vodafone Identified Huawei Security Flaw Decade Ago

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/elVXF4EUBWY/vodafone-identified-huawei-security-flaw-decade-ago

---

Cloud Microsoft, scoperto database non protetto con informazioni di 80milioni di famiglie Usa

E’ stato scoperto su un server cloud gestito da **Microsoft** un archivio di 24 gigabyte contenente i dati personali di 80 milioni di famiglie statunitensi.

L’archivio, non protetto, conteneva nomi, cognomi, date di nascita, indirizzi di residenza, genere, stipendio e stato civile di circa 80 milioni di famiglie USA (in totale in America le famiglie sono 128 milioni).

Nel database erano presenti inoltre dettagli sulla tipologia di abitazione delle famiglie coinvolte, con tanto di coordinate geografiche per localizzarla su una mappa, e un’indicazione che specificava se si trattasse di un edificio di proprietà o in affitto.

Considerata la natura dei dati e il nome attribuito ad alcuni campi del file come “member_code” e “score”, il sospetto è che potesse appartenere a qualche grande realtà del **settore**

immobiliare.

Fonte: vpnMentor

Il leak scoperto da vpnMentor

La falla è stata scoperta da una coppia di ricercatori israeliani del team di **vpnMentor** che ha affermato di aver scoperto il database non protetto mentre lavorava ad un progetto di mappatura web.

Chi possiede i dati sul server non è noto. Tuttavia, il misterioso hacker ha deciso di dettagliare tutte le informazioni per famiglia, anziché per singoli individui.

"*Questo database aperto è una miniera d'oro per ladri di identità e altri aggressor*i", ha dichiarato **vpnMentor**. Ad esempio, il tesoro di informazioni potrebbe aiutare gli hacker a rivolgersi ai ricchi o alle persone in base all'età.

La buona notizia è che il server è stato messo al sicuro. "*Abbiamo notificato al proprietario del database e stiamo prendendo le misure appropriate per aiutare il cliente a rimuovere i dati fino a quando non può essere adeguatamente protetto*", ha detto Microsoft in una dichiarazione. Tuttavia l'azienda, ha rifiutato di nominare il cliente.

I potenziali pericoli per la privacy

L'accesso al tuo nome completo può aiutare gli hacker a indovinare il tuo indirizzo email. Molte persone usano

nome.cognome@gmail.com come loro indirizzo email, quindi identificare la email è molto facile.

Questo scenario è solo la punta dell'iceberg. Gli indirizzi possono facilmente portare a numeri di telefono, rendendo le persone facili bersagli per le truffe di phishing. Le date di nascita e i codici postali sono risposte comuni alle domande di sicurezza. E la longitudine e la latitudine significano che le abitazioni possono essere individuate per eventuali furti.

https://www.key4biz.it/cloud-microsoft-scoperto-database-non-protetto-con-informazioni-di-80milioni-di-famiglie-usa/256182/

ImmuniWeb Launches Free Testing Tool for Website Security and PCI Compliance

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/z3CgsfrH93Y/immuniweb-launches-free-testing-tool-website-security-and-pci-compliance

---

Evasione fiscale, Garante Privacy: 'Si ai nuovi sistemi

ma nel rispetto dei cittadini’

Sì del **Garante per la privacy** alla sperimentazione di processi automatizzati per la lotta all’evasione fiscale, ma nel rispetto di precise garanzie a salvaguardia dei diritti dei cittadini. L’**Agenzia delle entrate** potrà iniziare ad utilizzare in via sperimentale modelli predittivi del rischio evasione attraverso la selezione automatizzata di posizioni fiscali dei potenziali evasori, anche mediante lo scambio di informazioni con amministrazioni estere.

L’Autorità ha adottato due distinti pareri su due schemi di provvedimento del Direttore dell’Agenzia delle entrate riguardanti rispettivamente contribuenti con incongruenze tra i redditi dichiarati e i loro rapporti bancari e finanziari, e cittadini che hanno intrattenuto rapporti con operatori finanziari all’estero non coerenti con le informazioni in possesso del fisco.

L’Autorità ha ritenuto idonee – anche sulla base della valutazione dei rischi effettuata dall’Agenzia dell’entrate – le garanzie individuate in termini organizzativi e di sicurezza informatica. Tali garanzie riguardano, in particolare: la qualità dei dati utilizzati per la selezione dei contribuenti; i tempi di conservazione dei dati; il diritto del contribuente a essere correttamente informato e di veder garantite adeguate modalità di coinvolgimento; la necessità di condurre controlli periodici sull’esattezza dei dati e di adottare misure volte a ridurre i rischi relativi a errate rappresentazioni della capacità contributiva, che potrebbero recare ingiustificati pregiudizi agli interessati.

All’Agenzia delle entrate – che avrà l’obbligo di inviare un avviso ai contribuenti sotto accertamento affinché provvedano a regolarizzare la propria posizione – l’Autorità ha chiesto

anche ulteriori garanzie per la condivisione con la Guardia di Finanza delle informazioni relative ai rapporti finanziari.

Giova ricordare che la selezione automatizzata dei contribuenti trova la sua base giuridica in una serie di norme nazionali, così come richiesto dal Regolamento Ue, che consente tali trattamenti nel caso in cui siano ammessi dalla normativa dello Stato membro, sulla base di precise misure a tutela delle persone, e siano autorizzati dall'Autorità garante.

Proprio alla luce del Regolamento europeo – allo scopo di evitare possibili discriminazioni o pregiudizi – i processi automatizzati devono garantire massima sicurezza e trasparenza, anche riguardo alla logica alla base degli algoritmi utilizzati.

L'Autorità seguirà da vicino la fase iniziale di sperimentazione per assicurare che vengano rispettate le misure individuate e sottoporrà a ulteriore analisi eventuali modifiche del modello predittivo utilizzato dall'Agenzia.

https://www.key4biz.it/evasione-fiscale-garante-privacy-si-ai-nuovi-sistemi-ma-nel-rispetto-dei-cittadini/256127/

Slack Lists Cybersecurity Risks Ahead of Going Public

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/FQh-OCzEHL8/slack-lists-cybersecurity-risks-ahead-going-public

I riders che chiedono diritti e poi non rispettano la privacy dei clienti: ‘Ecco i vip più tirchi di Milano’

Stupisce molto la pessima iniziativa del collettivo di rider precari “Deliverance Milano”, che ha pubblicato su Facebook l’elenco dei vip che ordinano cibo a casa, senza lasciare la mancia. Un autogol da parte di chi rivendica di ottenere i diritti base come lavoratore e poi vìola un altro diritto fondamentale delle persone, la privacy dei clienti. Arrecando anche un danno di immagine per le piattaforme di delivery per la quali lavorano in condizioni precarie.

“Questa è la nostra blacklist”, si legge nel post, *“un elenco di tutte le star e i vip che regolarmente ordinano con le app e non lasciano la mancia a nessun fattorino, nemmeno in caso di pioggia!”*

In questa lista, con 25 nomi, compaiono attori, presentatori, cantanti, calciatori, sportivi, musicisti, rapper, influencer.

Oltre alla violazione della privacy, anche la minaccia

Oltre alla violazione della privacy, il collettivo di rider ha lanciato anche una chiara minaccia, che dovrebbe essere subito vagliata dalle forze dell’ordine: *“Ricordatevi sempre una cosa clienti: entriamo nelle vostre case, vi portiamo il cibo e qualsiasi altra cosa vogliate, praticamente a tutte le ore del giorno, siamo in strada sotto la pioggia battente o*

sotto il sole cocente, senza assicurazione. Sappiamo tutto di voi. Sappiamo cosa mangiate, dove abitate che abitudini avete”.

Guerra tra poveri-ricchi-dati

Poi, nel post, è scattato anche l’attacco alle piattaforme del delivery: *«E come sappiamo noi tutto di voi, lo sanno anche le aziende del delivery. Queste piattaforme come sfruttano noi lavoratori senza farsi alcuno scrupolo, sfruttano anche voi, speculando e vendendo i vostri dati”.* Parlano del *“lato oscuro della Gig Economy”*, dove *“si produce valore in tutti i modi possibili, dal servizio di vendita del prodotto al trasporto a domicilio delle merci, fino alla mappatura dei dati, alla loro analisi e alla loro compravendita”.*

Quali i diritti richiesti

Nel post della pessima iniziativa il collettivo indica anche i diritti richiesti: *“non possiamo più prescindere dall’avere diritti sindacali, reddito incondizionato, salario minimo e una previdenza sociale adeguata”.* E la non tassazione delle mance: *“Pretendiamo che le nostre mance non vengano tassate, ad oggi viene trattenuta l’Iva quando il pagamento avviene (come la maggior parte delle volte) per mezzo del supporto di intermediazione digitale, quando dichiarate il contrario”*. Nel mirino anche i pagamenti in contante. *“E qualora fossimo costretti dal servizio aziendale a ricevere parte dei pagamenti in contante, pretendiamo un’indennità di cassa, perché già mentre siamo in consegna capita che veniamo aggrediti perché la gente cerca di derubarci o ci fregano le bici fuori dai palazzi e dai ristoranti, manca solo di venir rapinati e di rimetterci i soldi di tasca nostra”*.

A che punto siamo con i diritti richiesti dai riders della Gig economy?

In Italia nulla di concreto. La Giunta della Regione Lazio ha approvato la prima proposta di legge in Italia per la tutela e la sicurezza dei rider, i lavoratori della gig economy che consegnano il cibo. Il governatore Nicola Zingaretti, segretario del Pd, punta ad approvare la legge prima che lo faccia a livello nazionale **Luigi Di Maio**, che ha promesso di contribuire a risolvere il problema?

Nel frattempo, il 17 aprile scorso, il Parlamento europeo ha definito i diritti base dei lavoratori della Gig Economy. Ora toccherebbe farli applicare il prima possibile dalle aziende digitali (**Foodora, Uber Eats, Just Eat, Deliveroo, Glovo, Domino’s Pizza, Mooveda** e **Social Food**) che consegnano il cibo a domicilio, prima che alcuni lavoratori continuino a violare i diritti di altri lavoratori.

https://www.key4biz.it/i-riders-che-chiedono-diritti-e-poi-non-rispettano-la-privacy-dei-clienti-ecco-i-vip-piu-tirchi-di-milano/255979/