ARRAY

Avv. Carlo Piana

Piazza San Nazaro in Brolo 15
20122 Milano – Italy

tel +39 02 8718 6019
fax +39 02 700 419282

piana@array.eu
carlo.piana@pec.piana.eu

https://law.piana.eu
https://array.eu

VAT No. /P. IVA 06127180963

Milano, 11 dicembre 2018

Spett.le
IDM Südtirol - Alto Adige
Via Volta
39 100 Bolzano

Beacon e GDPR§

Executive summary

L'installazione ed il conseguente utilizzo di beacon tramite apposite app, consentendo potenzialmente la **geolocalizzazione** del fruitore del servizio, pone alcuni rilevanti problemi in relazione alla protezione dei dati personali (privacy) del medesimo, tipicamente il possessore di uno smatphone. Essi sono però profondamente diversi per l'**installatore** dei beacon rispetto allo **sviluppatore/fornitore** della relativa app.

Per i **titolari di una struttura** all'interno della quale i beacon verranno installati, l'obbligo sarà solo quello di **informare in modo chiaro e visibile** i propri utenti del fatto che nell'area sono installati i dispositivi, con l'espresso avvertimento di disattivare il Blutooth se vogliono evitare anche la remota ipotesi di essere geolocalizzati.

Agli **sviluppatori/ fornitori di una Beacon App**. Il GDPR (Regolamento UE 2016/679) richiede che i prodotti ed i servizi debbano essere **progettati** fin dall'inizio con caratteristiche in grado di garantire sempre agli interessati che i loro dati siano trattati lecitamente (principi di *"**privacy by design and by default**"*).

Per le Beacon App una **rilevante** differenza, ancora, si rinviene nel caso in cui i dati di geolocalizzazione siano trattati solo **all'interno dell'app**, senza che vi sia registrazione o un utilizzo dei medesimi diverso dal mero funzionamento istantaneo dell'app. Non configurandosi un trattamento di dati sarà infatti sufficiente che venga data all'interessato un'**informativa**

§ Il testo è stato redatto dall'Avv. Elisabetta Fabio con la supervisione, indicazioni e revisione dell'Avv. Carlo Piana.

efre·fesr Südtirol · Alto Adige
Europäischer Fonds für regionale Entwicklung
Fondo europeo di sviluppo regionale
EUROPEAN UNION
AUTONOME PROVINZ BOZEN SÜDTIROL
PROVINCIA AUTONOMA DI BOLZANO ALTO ADIGE

Titolo: Beacon Südtirol - Alto Adige
CUP: B31H17000060001

completa in merito all'utilizzo, o non utilizzo, che dei suoi dati personali viene fatto e i dati dovranno di regola essere **cancellati** il più possibile dopo il loro utilizzo.

Numerosi e più complessi saranno invece gli adempimenti da porre in essere nel caso in cui la Beacon App sia solo un *frontend* ed i dati transitino dall'app verso un ***backend* in cloud**. In questo caso il titolare del trattamento dei dati personali oltre a dare all'interessato un'**informativa completa** in merito all'utilizzo che prevede di fare dei dati raccolti ed a individuare ed attuare tutte le **misure tecniche ed organizzative** idonee a **minimizzare il rischio** connesso al trattamento dei dati, in relazione al concreto utilizzo dei dati raccolti tramite la singola Beacon App considerata (finalità del trattamento, ambito di raccolta dei dati, eccetera) dovrà valutare se attuare anche **ulteriori specifici adempimenti**.

In particolare, ***potrebbe*** rendersi in taluni casi necessaria, per esempio nel caso in cui i dati siano raccolti su larga scala, se il titolare è un ente o un'autorità pubblica o quando si ritenga che il rischio per il trattamento dei dati sia da considerarsi elevato, la **nomina di un responsabile della protezione dei dati** (o Data Protection Officer - **DPO**).

Inoltre, nel caso di dati personali raccolti tramite l'utilizzo di Beacon App si ricade nell'uso di una tecnologia da considerarsi "innovativa" e dunque le cui implicazioni non sono state sufficientemente testate. È assai verosimile che si sia obbligati, **prima di procedere al trattamento** dei dati, consultato il DPO, ad effettuare una **valutazione d'impatto** sulla protezione dei dati personali – **DPIA** (art. 35 del GDPR). Questa valutazione di impatto dovrà essere, avviata fin dalla **fase di progettazione** del trattamento e poi continuamente riesaminata e rivalutata da parte del titolare.

Nell'ipotesi in cui, una volta effettuata la DPIA, il titolare del trattamento ritenga di non essere in grado di trovare misure sufficienti per ridurre il rischio ad un livello accettabile, dovrà inoltre **consultare preventivamente il Garante** competente per ottenere indicazioni su come gestire il rischio residuale (art. 36 GDPR). Il procedimento potrebbe anche essere di **non breve durata**. All'esito il Garante potrà indicare le **misure ulteriori** eventualmente da implementare a cura del titolare del trattamento ma potrà anche eventualmente adottare le **misure correttive** al trattamento che ritiene più idonee, finanche ad arrivare a **vietare** il trattamento dei dati per cui la consultazione è stata richiesta.

Le **valutazioni** che, per il principio dell'*accountabilty* lo sviluppatore dovrà compiere in merito alle concrete misure da adottare ed adempimenti da porre in essere sono quindi molto delicate e richiedono di essere **attentamente ponderate**, anche in considerazione del fatto che all'inosservanza di quanto previsto dal GDPR sono connesse **sanzioni amministrative** che possono arrivare a 10 milioni di euro e, se si tratta di un'impresa, fino al 2% del fatturato.

***

Discussione

1. Lo scenario: il progetto "Beacon Südtirol-Alto Adige"

Il progetto, avviato nel maggio del 2018 e finanziato dal programma ERDF coordinato dal Ecosystem ICT & Automation del IDM Südtirol - Alto Adige e dalla Divisone 9.0 della Provincia Autonoma di Bolzano, si pone come obiettivo la creazione di un ambiente favorevole per lo sviluppo di progetti e prodotti innovativi tramite l'installazione di una rete di beacon.

A tal fine si prevede in particolare l'installazione di 3.500 beacon distribuiti su tutto il territorio del Sud Tirolo ed il parallelo sviluppo di una "*Open Source library*" che mapperà i beacon installati, nonché lo sviluppo di un "Open Source web tool" e di un "*Open Source app*" per gestire la rete di beacon.

Il progetto si basa quindi interamente sull'utilizzo di dispositivi beacon che consentono, attraverso la tecnologia Bluetooth,[1] di trasmettere piccoli messaggi, entro brevi distanze, constando di un presentatore o trasmettitore (dispositivo beacon) e un ricevitore che rileva i messaggi dei sensori beacon, attivando, ove programmate, specifiche funzioni.[2]

L'informazione fornita dai beacon consiste in un semplice UUID (*Universally Unique Identifier*), ovvero un identificatore univoco. Di per sé il beacon non ha alcuna logica intrinseca, tutta la logica e le informazioni devono essere dedotte da fonti e applicazioni esterne. Il ricevitore, rileva la presenza dei trasmettitori entro una distanza che varia tra i 3 e i 60 metri, e dunque può utilizzare questa informazione per compiere attività arbitrariamente determinate da chi predispone l'applicazione.

Allo stato attuale risulta che i beacon saranno installati su **supporti fissi** e non quindi su elementi dinamici (quali, ad esempio, mezzi di trasporto) ed è sulla base di questa premessa che l'analisi verrà svolta. Qualora vi fosse la necessità di installarli su veicoli o su oggetti trasportabili, l'analisi comporterebbe la possibilità di monitorare il portatore, con implicazioni privacy molto più complesse ed estese.

2. Le questioni legali connesse alla tutela della privacy

Da un punto di vista legale si pone il problema di prevedere quali possano essere le problematiche connesse all'installazione ed al conseguente utilizzo dei beacon in relazione alla protezione dei dati personali dell'utente finale (tipicamente, il possessore di un apparato portatile, come uno smartphone).

Vi può infatti essere un rischio nel trattamento dei dati personali dell'utente dei servizi della rete di beacon e la natura e la portata di tale rischio dipende strettamente da diverse variabili tra cui in primo luogo la **finalità** dell'uso dei dati raccolti, con il correlativo

---

1 Bluetooth è un marchio registrato di Bluetooth SIG, Inc.

2 Questa la definizione di beacon fornita dal Garante per la protezione dei dati personali nel provvedimento n. 29 del 25 gennaio 2018 "Verifica preliminare. Raccolta di dati attraverso il monitoraggio a distanza dei pazienti non autosufficienti".

rischio derivante dal trattamento dei dati personali[3] dell'utente a scopo di **profilazione**[4], soprattutto con riferimento alla **geolocalizzazione** ed alle **preferenze personali** del medesimo.

Alla luce della normativa sul trattamento dei dati personali vigente (Regolamento UE 2016/679 del 27 aprile 2016 – GDPR,[5] D.lgs 196/2003 come modificato dal D.lgs 101/2018 e provvedimenti del Garante per la protezione dei dati personali), si cercherà di individuare quali possano essere, sulla base delle informazioni disponibili, delle possibili linee guida sia per coloro che installeranno all'interno delle proprie strutture questa tecnologia sia per coloro che intendano creare ed utilizzare delle app che la sfruttino.

Ai fini dell'analisi dei rischi connessi al progetto è necessario preliminarmente distinguere gli enti che installeranno i beacon nelle proprie strutture da coloro che realizzeranno o commissioneranno la realizzazione delle app che utilizzino gli stessi beacon, potendo questi ultimi essere sia i medesimi detentori dell'infrastruttura che soggetti terzi.

3. L'installazione dei beacon

Per gli enti che installeranno i beacon all'interno delle proprie strutture il quesito che si pone è se essi debbano o meno **informare** le persone che interagiranno con questa tecnologia semplicemente accedendo all'area, del fatto che nell'area in questione sono installati dei beacon, a prescindere dalla circostanza che sia stata sviluppata o meno un app dedicata e che l'utente decida liberamente, laddove questa sia disponibile, di scaricarla e di utilizzarla.

Occorre distinguere alcune ipotesi.

Nell'ipotesi in cui l'utente acceda con un device ed il Bluetooth attivo ad un'area in cui sono presenti beacon, potrebbe ricevere il messaggio inviato dal dispositivo trasmittente a lui più prossimo, ma il dispositivo non dovrebbe essere in grado di interpretatre l'input inviato dal beacon se non vi è installata una app che gli consenta di utilizzare l'informazione così ricevuta. In questa ipotesi, si potrebbe ritenere che non vi sia alcun trattamento rilevante di dati personali[6] e, quindi, concludere per l'esclusione della necessità di informare l'utente della presenza dei dispositivi.

Non è possibile tuttavia escludere a priori che l'utente abbia installato sul proprio device, anche a sua insaputa, app di terze parti che dialoghino con i beacon o che vi siano (o siano in futuro sviluppati) dispositivi sensibili ai beacon anche senza la necessità di avere

---

3 Dati personali definiti come *"qualsiasi informazione riguardante una persona fisica identificata o identificabile (...)"* ex art. 1, c. 1, 1) GDPR.

4 Profilazione intesa come *"qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"* ex art. 1, c. 1, 4) GDPR.

5 Nel testo useremo spesso la versione inglese dei termini del GDPR, incluso lo stesso acronimo, perché più precisi e rigorosi di quelli della traduzione italiana.

6 Secondo la definizione di "trattamento" indicata dall'art. 4 c. 1 punto 2) del GDPR.

installato una app abilitata:[7] se così fosse, avremmo un trattamento dati rilevante ai sensi della normativa di cui sopra. Stando così le cose, non si può escludere a priori che terze parti possano ricavare informazioni georeferenziate relative all'utente per il solo fatto che questi sia entrato con il proprio dispositivo nel raggio di trasmissione di un beacon come, per esempio, nell'ipotesi in cui abbia installato sul cellulare una app che potrebbe, anche a sua insaputa, interagire con i beacon se il Bluetooth è acceso.

Questa considerazione è tanto più vera se si considera che uno degli obiettivi del progetto è la creazione di una banca dati liberamente accessibile sui beacon installati sul territorio e quindi l'incrocio dei due dati potrebbe rendere effettivamente geolocalizzabile l'utente persino nell'ipotesi in cui questi abbia la localizzazione disattivata.

3.1.1. → Suggerimenti

Alla luce di queste considerazioni appare certamente opportuno, quando non addirittura necessario, che coloro che installeranno presso le proprie strutture i beacon **ne comunichino in modo chiaro la presenza agli utenti**, avvisandoli:

1. della **presenza** dei dispositivi;
2. del fatto che vi è una **banca dati liberamente consultabile** con la mappa della dislocazione dei dispositivi sul territorio, oltre a poter esistere altri servizi che sistematicamente raccolgano e cataloghino le stesse informazioni, georeferenziandole;
3. che i medesimi beacon potrebbero **interagire** con alcune app installate sul loro cellulare rendendoli geolocalizzabili;
4. che laddove volessero evitare ogni "rischio" di essere geolocalizzati è necessario che **spengano** il Bluetooth;
5. che ulteriori e più approfondite informazioni, ed il link alla mappa dei dispositivi, possono essere trovate sul sito dell'ente installatore, accessibile eventualmente anche attraverso un QR code da posizionarsi sull'informativa.[8]

Nell'ipotesi in cui sia stata anche sviluppata una app per utilizzare i beacon installati ma che questa medesima app sia stata sviluppata da terze parti e non dallo stesso installatore, l'informativa dovrà essere accompagnata dal un ulteriore avviso agli utenti che specifichi, perlomeno che:

1. vi è la possibilità di scaricare e installare una app che consente di ottenere un determinato risultato tramite l'utilizzo dei beacon;
2. l'app in questione è di **terze parti** e che l'installatore non è in alcun modo responsabile di quanto contenuto nell'app.

---

7 Sulla piattaforma Google Beacon Platform è per esempio indicato un servizio di Nearby Notification che non prevede la preventiva installazione di alcuna app dedicata. Il servizio, peraltro, non parrebbe avere soddisfatto le aspettative e Google ha annunciato che verrà terminato dal mese di dicembre 2018 in favore di un servizio simile ma reso tramite una app.

8 Nel provvedimento n. 551 del 21 dicembre 2017 relativo a "Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria" il Garante per la Protezione dei Dati Personali individua queste modalità informative come valide e sufficienti ad informare gli utenti.

4. Lo sviluppo di Beacon App

Le problematiche giuridiche più rilevanti connesse al tema del trattamento dei dati personali e all'utilizzo dei beacon sono tuttavia sicuramente legate alle **app** ad essi dedicate e possono variare anche notevolmente in funzione della finalità per cui tali app sono sviluppate, dell'utilizzo dei dati raccolti, dell'ampiezza e tipologia di area all'interno della quale i beacon interessati dall'app sono installati, eccetera. L'analisi si limita, naturalmente, ad esaminare le finalità per cui, allo stato attuale, vi è interesse tra i partecipanti al progetto a sviluppare le Beacon App (sistemi di *reccomendation*, sistemi di *gamification*, sistemi di navigazione interna, sistemi per migliorare l'esperienza dell'utente fornendo informazioni più specifiche, sistemi di controllo dei flussi dei visitatori, ...), fermo restando che sarà, poi, necessario scendere nel dettaglio di ogni singola app per verificare che non vi siano profili di rischio specifici che siano sfuggiti ad un'analisi più generale.

Il GDPR richiede, infatti, che il produttore/sviluppatore rispetti i principi di "*privacy by design and by default*"[9] (in base al quale i prodotti e i servizi devono essere progettati fin dall'inizio con caratteristiche in grado di garantire sempre agli interessati che i loro dati siano trattati lecitamente) attraverso un approccio "*risk based*", tramite, cioè, una preventiva valutazione dell'impatto che la tecnologia adottata avrà sulle libertà ed i diritti degli interessati.

Con riferimento allo sviluppo delle Beacon App e ai dati personali raccolti occorre distinguere il caso in cui i dati personali siano trattati dalla Beacon App solo **all'interno dell'app** senza che vi sia una **registrazione** o un utilizzo **secondario** dei medesimi dal caso in cui l'app sia solo un'interfaccia e vi sia un *backend* in cloud dove transitano i dati.

Nel primo caso infatti non si delineerebbe un trattamento di dati, considerato che questi non verrebbero né salvati né trasmessi altrove né utilizzati per un fine secondario diverso dal mero funzionamento istantaneo dell'app sul solo dispositivo dell'interessato. Ciò a condizione che questi dati siano isolati e non accessibili da altre applicazioni, se registrati.

Nella seconda ipotesi è invece evidente che l'app si configuri solo come *frontend* ma che i dati in ingresso transitino dall'app verso un *backend* dove vengono raccolti.

In questo caso per valutare il rischio e poter quindi impostare un sistema che preveda la tutela della "*privacy by design*" e quindi fin dalla sua progettazione, come richiesto dalla norma, sarà essenziale **definire**:

- lo spazio fisico all'interno del quale i beacon sono installati;
- che tipo di dati saranno raccolti;
- con quale finalità saranno raccolti i dati;
- per quanto tempo saranno conservati;
- di conseguenza, che tipo di misure di tecniche e organizzative si prevede di porre in essere per minimizzare il rischio.

9 Principio previsto dall'art. 25 GDPR.

4.1. Principi generali sulla minimizzazione dei rischi

La normativa sulla privacy impone alcune cautele per la minimizzazione dei rischi e la riduzione delle fonti di attacco a tutela dei diritti degli interessati.

4.1.1. Definire il contesto di raccolta

Individuare il **contesto** all'interno del quale la presenza dei beacon è **rilevata** e i realtivi dati sono **conservati** è essenziale al fine di valutare se si debba considerare la raccolta dati come effettuata su larga scala.

La nozione di "larga scala" è attualmente data dal parere del Gruppo di lavoro articolo 29 - WP29[10] (oggi EDPB), che raccomanda di tenere in considerazione:

- il **numero** dei soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il **volume** dei dati e/o le diverse tipologie di dati oggetto del trattamento;
- la **durata** ovvero la **persistenza** dell'attività di trattamento;
- la **portata geografica** dell'attività di trattamento.[11]

In base a questi criteri, si può ritenere che la raccolta di dati effettuata all'interno di uno spazio chiuso ma accessibile al pubblico, come potrebbe per esempio essere un'area espositiva, o aperto, come potrebbe ad esempio essere un impianto sciistico, potrebbe rientrare nel concetto di **larga scala**.

Da tale qualificazione discendono peraltro alcune rilevanti conseguenze ed obblighi per il Titolare del trattamento (o il Responsabile del trattamento) che dovrà:

i) designare un responsabile della protezione dei dati (o data protection officer - **DPO**)[12], una figura indipendente prevista dal GDPR, cui competono alcuni specifici compiti per assicurare il rispetto delle norme a tutela del trattamento dei dati.[13]

ii) effettuare una previa valutazione di impatto (**DPIA**) prevista dall'art. 35 del GDPR.

4.1.2. Individuare la tipologia di dati raccolti

Con riferimento alla tipologia di dati raccolti, interpretati e conservati, la rete di beacon permetterà in primo luogo di rilevare il dato riguardante la **geolocalizzazione** di ogni singolo utente in un dato momento ed anche di tracciare i suoi spostamenti nello spazio.

Questo singolo dato, se analizzato in modo aggregato facendo ricorso a tecniche di profilazione, potrebbe essere rivelatore di molte informazioni riguardanti l'interessato, come per esempio preferenze, comportamenti, interessi e posizioni personali.

---

10 Ora sostituito dal Comitato Europeo per la protezione dei dati – EDPB – è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.

11 Si veda in particolare la spiegazione contenuta nel parere del WP29 sulla limitazione della finalità – 13/EN WP 203, pag. 24.

12 Art. 37 c. 1, b) GDPR.

13 Si vedano i compiti elencati all'art. 39 GDPR.

Analizzando per esempio il numero di accessi che in un anno un soggetto compie all'interno di un determinato luogo, per esempio un museo, si potrà concludere che quel determinato soggetto è un frequentatore assiduo di eventi culturali e magari, analizzati i dati, che predilige particolarmente le mostre di una determinata corrente pittorica piuttosto che un'altra.

Inoltre, poiché i beacon rilevano la posizione del soggetto ricevente con un grado di prossimità molto elevato, sarà in ipotesi anche possibile calcolare il tempo di permanenza dell'utente davanti ad un determinato dispositivo beacon e di conseguenza, volendo continuare a seguire l'esempio precedente, davanti ad una determinata installazione traendone quindi tutte le conseguenze del caso.

Proprio per la capacità che i dati relativi alla localizzazione di un dispositivo mobile hanno di rivelare dettagli della vita privata dell'utilizzatore si dovrà predisporre **un'idonea informativa** e, laddove necessario, prevedere il rilascio del **consenso dell'interessato**.[14]

4.1.3. Definire le finalità per cui i dati saranno raccolti

Il GDPR richiede, inoltre, di indicare specificamente le finalità del trattamento dei dati, perché un trattamento eseguito al di fuori delle finalità dichiarate, costituisce un illecito trattamento di dati, con applicazione della relativa disciplina sanzionatoria e risarcitoria.

Inoltre, definire preventivamente le finalità per cui i dati personali sono raccolti è essenziale per identificare il grado di rischio connesso al trattamento e valutare di conseguenza quali siano le misure concrete da adottare per mitigarlo.

Usare il dato relativo alla posizione di un utente rilevato tramite la rete di beacon con la sola finalità di fornirgli indicazioni sulla propria localizzazione all'interno di una struttura ed indicazioni più precise sulla navigazione interna alla medesima struttura è infatti una finalità ben diversa e con un rischio connesso al trattamento dei medesimi dati altrettanto diverso rispetto ad un sistema che raccolga i dati con la finalità di elaborarli per fornire all'utente suggerimenti personalizzati in merito alle sue scelte future nei più svariati campi.

4.1.4. Definire un tempo di conservazione dei dati

Il GDPR richiede, inoltre, che sia stabilito preventivamente il periodo di conservazione dei dati personali, limitandolo al minimo strettamente necessario[15].

---

14 Il consenso deve sempre essere espresso. La necessità di consenso dipende dalle finalità del trattamento. Non è possibile dare una elencazione di quali trattamenti necessitino del consenso. Ad esempio, se il trattamento è necessario per l'esecuzione di prestazioni contrattuali, il consenso non è necessario. Se è necessario per soddisfare un interesse prevalente del titolare del trattamento, il consenso non è necessario.

15 Il titolare del trattamento deve quindi comunicare nell'informativa data all'interessato al momento della richiesta del consenso per la raccolta dei dati il periodo di conservazione degli stessi oppure, se ciò non è possibile, i criteri utilizzati per determinare tale periodo e, in ogni caso, per assicurare che i dati personali non siano conservati più a lungo del necessario, dovrebbe stabilire un termine per la cancellazione o per la verifica periodica.

I dati non rilevanti vanno scartati immediatamente e non conservati (principio di minimizzazione dell'*attack footprint*).

Se, per esempio, la finalità della raccolta dati e del loro trattamento sarà solo quella di monitorare gli sciatori presenti su alcune piste al fine di garantire la massima sicurezza e prontezza di intervento in caso di incidenti, il dato raccolto dovrà essere conservato solo fino all'uscita dell'utente dagli impianti o alla fine della giornata e poi dovrà essere cancellato.

Se al contrario i dati che verranno raccolti all'interno di un impianto sciistico saranno trattati con la finalità di monitorare per esempio il numero di accessi di un utente agli impianti durante una stagione con lo scopo di proporgli un abbonamento personalizzato per la stagione sciistica successiva, i dati raccolti – previo suo consenso esplicito – potranno essere conservati per tutta la durata della stagione o anche oltre, se così sarà determinato nella relativa informativa.

4.1.5. Individuare le misure di tecniche e organizzative più appropriate in relazione al caso concreto per minimizzare il rischio

Il GDPR richiede, inoltre, nell'ambito dei principi di "*privacy by design* e *privacy by default*" di cui all'articolo 25 sopra illustrati, che il titolare del trattamento metta in atto misure tecniche ed organizzative adeguate al rischio e la valutazione della loro idoneità sarà rimessa, caso per caso, al titolare del trattamento, sulla base di una preventiva attività di valutazione del rischio.

Ancora una volta quindi per individuare concretamente quali possano essere le misure da adottare nel singolo caso, ad esempio valutare di prevedere la cifratura e pseudonimizzazione dei dati personali o una tra le altre misure di sicurezza suggerite dal GDPR,[16] è essenziale avere riguardo alle concrete circostanze, modalità e finalità con cui i dati verranno raccolti e trattati.

Così in via teorica si potrebbe infatti ritenere ad esempio che nel caso in cui la finalità del trattamento sia la profilazione dell'utente con riferimento ai suoi interessi personali la pseudonimizzazione del dato sia da ritenersi una misura di sicurezza necessaria al fine di minimizzare il rischio, mentre nel caso in cui il dato venga raccolto al solo fine di fornire un'informazione migliore su come orientarsi all'interno di una struttura tale precauzione possa non servire.

In questo contesto, diventa imprescindibile garantire la sicurezza della rete beacon da violazioni e/o abusi della stessa, prevedendo idonee misure di cyber security, prevedendo ad esempio un meccanismo che prevenga tentativi di autenticazioni non autorizzate, assegnando ad ogni beacon una password univoca, cifrando il valore major e minor trasmesso dai beacon etc.

---

16 In particolare l'art. 32 GDPR prevede che, tra le altre misure di sicurezza da porre in essere per garantire un livello di sicurezza adeguato al rischio vi sia oltre a: *"a) la pseudonimizzazione e cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".*

4.1.6. → Suggerimenti

Alla luce dei principi del GDPR che, come sinteticamente sopra delineati, impongono al titolare del trattamento di adottare delle misure che concretamente minimizzino il rischio connesso al trattamento dei dati stessi, non è possibile delineare a priori ed in via astratta le singole specifiche azioni da porre in essere e le misure da adottare per ipotesi eterogenee tra loro, quali ad esempio lo sviluppo di un app che utilizzi i dati per creare un sistema di raccomendation e quello di un app che invece utilizzi i dati per monitorare solo il flusso dei visitatori di un'area o, invece, che sia di supporto alla navigazione interna all'area medesima.

Al fine di sviluppare una Beacon App conforme ai requisiti del GDPR è però sicuramente necessario, come si è detto, definire preventivamente:

1. in che **ambito** verranno raccolti i dati;
2. quale **tipo** di dati saranno raccolti (tramite le inferenze del caso);
3. con quale **finalità** i dati saranno raccolti;
4. per quanto **tempo** è necessario che i dati raccolti siano conservati;
5. se si prevede di **comunicare i dati** a soggetti **terzi**;
6. dove (e come, per ciascuna finalità) verranno **conservati** i dati.

Solo una volta definiti questi aspetti sarà quindi possibile valutare il rischio connesso al trattamento dei dati e determinare, di conseguenza, quali concrete misure tecniche ed organizzative debbano essere adottate per garantire un livello di sicurezza adeguato al rischio.

Volendo tuttavia cercare di individuare un possibile quadro giuridico di riferimento comune in relazione al trattamento dei dati personali raccolti tramite le Beacon App, si evidenziano le seguenti ulteriori informazioni utili.

4.1.7. Acquisire il consenso dell'interessato (eventuale)

Il Regolamento generale sulla protezione dei dati personali individua diverse ipotesi che rendono lecito il trattamento dei dati.[17] Nel caso (eventuale) in cui però la base giuridica per il trattamento dei dati acquisiti per mezzo delle Beacon App sia il consenso dell'interessato,[18] è necessario che il Titolare del trattamento acquisisca un previo consenso da parte dell'interessato al trattamento dei propri dati personali.[19]

Il Titolare del trattamento deve inoltre essere in grado di dimostrare che l'interessato ha prestato il proprio consenso in tal senso,[20] il che concretamente si traduce nella necessità che il consenso sia acquisito tramite uno **specifico processo** a ciò destinato all'interno della app e che sia preliminare all'avvio dell'app stessa. Di tale consenso si dovrà poi **tenere traccia** e quindi è necessario che sia **conservato**.

17 Art. 6 GDPR.
18 Cfr. nota 14
19 Art. 6, c. 1, a) GDPR.
20 Art. 7, c. 1 GDPR.

La richiesta di consenso dovrà inoltre essere presentata in **modo chiaro** e con un **linguaggio semplice** ed essere accompagnata dall'informazione che l'interessato potrà in ogni momento revocare il consenso prestato.[21]

È opportuno inoltre che sia reso **ben distinguibile** il consenso al trattamento dei dati che viene richiesto come condizione per il funzionamento dell'app dal consenso al trattamento di dati che, pur essendo richiesto, non è necessario all'esecuzione del servizio.[22]

Nella fase della richiesta del consenso dovrà essere poi inserita una dichiarazione da parte dell'interessato di avere un'età maggiore almeno di sedici anni e andrà valutata con cautela l'ipotesi di inserire o meno un meccanismo di richiesta del consenso al trattamento dei dati del minore al titolare della responsabilità genitoriale per il caso in cui il soggetto che utilizza la Beacon App abbia meno di sedici anni.[23]

4.1.8. Fornire un'informativa all'interessato

L'articolo 13 del GDPR prevede dettagliatamente il contenuto dell'informativa che dovrà essere fornita all'interessato nel momento in cui i dati personali sono ottenuti.[24]

---

21 Art. 7, cc. 2 e 3 GDPR.

22 Art. 7, c. 4 GDPR.

23 Art. 8 GDPR.

24 Essa dovrà contenere in particolare e per quanto qui di interesse:

- l'**identità e i dati di contatto del titolare del trattamento** e, ove applicabile, del suo rappresentante;i **dati di contatto del responsabile della protezione dei dati** (DPO);
- le **finalità del trattamento** cui sono destinati i dati personali nonché la **base giuridica del trattamento** (solitamente il consenso dell'interessato);
- gli eventuali **destinatari** o le eventuali categorie di destinatari dei dati personali;
- se il titolare del trattamento ha intenzione di **trasferire dati personali ad un paese terzo** (...);
- il **periodo di conservazione dei dati personali** oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del **diritto dell'interessato** di chiedere al titolare del trattamento l'**accesso ai dati personali** e la **rettifica** o la **cancellazione** degli stessi o la **limitazione del trattamento** che lo riguardano o di **opporsi al loro trattamento**, oltre al **diritto alla portabilità dei dati**;
- l'esistenza del **diritto di revocare il consenso al trattamento** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il **diritto di proporre reclamo a un'autorità di controllo**;
- **se la comunicazione** di dati personali **è un obbligo legale o contrattuale** oppure un **requisito necessario per la conclusione di un contratto**, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'**esistenza di un processo decisionale automatizzato**, compresa la **profilazione**, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

In linea generale i principi di trattamento corretto e trasparente implicano che l'interessato sia informato **dell'esistenza** del trattamento e delle sue **finalità** nonché del **diritto di accedere** ai dati personali raccolti, chiederne la **rettifica**, la **cancellazione** e la **portabilità** ed anche che l'interessato sia **informato della possibilità di revocare** sempre il **consenso**.

Nel concreto ciò implica che sia previsto fin dall'inizio da parte del titolare del trattamento un processo interno che renda effettivamente possibile per l'interessato l'esercizio dei suoi diritti in merito ai dati personali raccolti.

Il titolare del trattamento dovrà inoltre fornire all'interessato eventuali ulteriori informazioni, quali ad esempio il **periodo di conservazione** dei dati, necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze ed il contesto specifici in cui i dati personali sono trattati.

Inoltre, l'interessato dovrebbe essere informato dell'esistenza di una profilazione (se esiste) e delle conseguenze della stessa come anche dell'eventuale **obbligo** di fornire i dati personali e delle **conseguenze** in cui incorre se si rifiuta di fornirli.[25]

4.2. Nominare un responsabile della protezione dei dati – DPO

Come si è anticipato, nel caso in cui le attività principali[26] del titolare del trattamento consistano in trattamenti di dati che, per natura, ambito di applicazione o finalità, richiedono un "monitoraggio regolare e sistematico degli interessati su larga scala", il titolare del trattamento ed il responsabile del trattamento devono necessariamente nominare un responsabile della protezione dei dati (o **DPO** - Data Protection Officer).[27]

Tale figura dovrebbe essere una **persona**, indifferentemente un dipendente del titolare o del responsabile del trattamento oppure un soggetto esterno che agisca sulla base di un contratto di servizi, che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati e che vigili sul rispetto a livello interno del regolamento generale per la protezione dei dati.

Il regolamento generale per la protezione dei dati personali assegna al DPO dei **compiti**[28] specifici e prevede che questi debba svolgere le proprie funzioni in maniera indipendente rispetto al titolare ed al responsabile del trattamento.[29]

Anche al di là dell'ipotesi tassativamente prevista dalla norma per la nomina del DPO di cui si è detto sopra, e quindi anche nel caso in cui il trattamento dei dati non sia effettuato su larga scala, la nomina di un DPO potrebbe essere comunque consigliabile, anche se non obbligatoria.

---

25 Considerando 60 del GDPR.

26 Il considerando 97 del GDPR specifica che le attività principali del titolare del trattamento riguardano le attività primarie di questo ed esulano quindi dal trattamento dei dati personali come attività accessoria.

27 Art. 37, c. 1, par. b).

28 L'art. 39 GDPR individua i compiti del responsabile della protezione dei dati.

29 Art. 38 GDPR.

Ed infatti in tutte le ipotesi in cui il rischio per il trattamento dei dati sia da considerarsi elevato la nomina da parte del titolare del trattamento di una figura specialistica che vigili in modo indipendente sull'applicazione ed il rispetto della normativa privacy dall'interno rende sicuramente il processo di gestione dei dati più sicuro e certo, contribuendo a dare un contenuto concreto al principio, che come si è detto ispira tutto il GDPR, di responsabilizzazione del titolare del trattamento, aiutando quest'ultimo a dimostrare che sono state adottate misure adeguate per garantire il rispetto del medesimo regolamento.

4.3. Effettuare la valutazione di impatto sulla protezione dei dati – DPIA

Una volta che il titolare del trattamento abbia valutato il rischio e previsto l'adozione delle più opportune misure tecniche ed organizzative per la sua mitigazione, potrebbe in linea teorica iniziare il trattamento dei dati.

Nel caso di dati personali raccolti tramite Beacon App appare però opportuno che prima di procedere al trattamento dei dati il titolare del trattamento, consultato anche il DPO, effettui una **valutazione dell'impatto** dei trattamenti previsti sulla protezione dei dati personali in conformità a quanto previsto dall'articolo 35 del GDPR.

Infatti alla luce del disposto normativo,[30] delle linee guida elaborate dal WP29[31] e da ultimo anche dall'analisi dell'elenco di tipologie di trattamenti soggetti al requisito della valutazione di impatto sulla protezione dei dati pubblicata dal nostro Garante per la protezione dei dati personali,[32] si deve ritenere che il trattamento in questione presenti un rischio elevato per i diritti e le libertà delle persone fisiche e la valutazione preventiva debba essere svolta.

Per valutare nel caso concreto quando un rischio possa essere considerato "elevato" le linee guida elaborate dal WP29 hanno infatti individuato nove criteri che, benché non esaustivi, sono il punto di partenza per svolgere questo tipo di analisi.

Peraltro le stesse linee guida prevedono che "maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione

---

30 L'art. 35, c. 1 GDPR stabilisce infatti che "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

31 Linee guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 del 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (WP 248 rev.01).

32 Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del regolamento (UE) n. 2016/679" del 11 ottobre 2018 n. 467 e relativo "Allegato 1".

d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare".[33]

Ciò posto, pare che con riferimento al trattamento dei dati raccolti tramite le Beacon App possano venire in rilievo quanto meno i seguenti criteri elaborati nel WP 248 rev. 01, che sono state pari-pari riprese anche dal Garante italiano[34] come prescrittive per la necessità di effettuare una valutazione di impatto:

- criterio n. **3**: **monitoraggio sistematico** trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la **sorveglianza** sistematica su larga scala di una zona **accessibile al pubblico";**[35]
- criterio n. **4**: dati **sensibili** o dati aventi carattere **altamente personale**. Oltre ai dati considerati altamente personali per definizione (ad esempio informazioni sulle opinioni politiche delle persone, nonché dati personali relativi a condanne penali, etc.), le linee guida stabiliscono che vi sono alcune categorie di dati che possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche e tra questi dati considerati essere sensibili vengono indicati anche i dati relativi all'ubicazione, la cui raccolta influenza l'esercizio di un diritto fondamentale e cioè la **libertà di circolazione**;
- criterio n. **5**: trattamento di dati su **larga scala** di cui si è già detto nel precedente paragrafo 4.2;
- criterio n. **8**: uso **innovativo** o applicazione di **nuove soluzioni tecnologiche** od organizzative. Il regolamento generale sulla protezione dei dati chiarisce[36] che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto",[37] può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. "Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" (**IoT**) potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati".[38]

Alla luce di quanto sopra appare quindi evidente che vi possa essere **più di criterio che soddisfa il trattamento dei dati raccolti tramite le Beacon App** e quindi che

33 WP 248 rev.01, *cit.*, pag. 12.

34 "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto" allegato al provvedimento n. 467 dell'11 ottobre 2018 del Garante per la protezione dei dati.

35 Art. 35, c. 3, lett. c) GDPR.

36 Articolo 35, c. 1 e considerando 89 e 91.

37 Considerando 91.

38 Così WP 248 rev.01, *cit.*, pag. 11.

faccia propendere per la qualificazione del rischio connesso al trattamento come elevato e richiedente pertanto che sia effettuata una valutazione di impatto sulla protezione dei dati.

Dal punto di vista organizzativo è inoltre bene tenere presente che tale valutazione di impatto deve essere:

- avviata "il prima possibile nella fase di progettazione del trattamento anche se alcune delle operazioni di trattamento non sono ancora note";[39]
- continuamente riesaminata e rivalutata con regolarità da parte del titolare del trattamento, nel contesto dei suoi obblighi generali di responsabilizzazione;
- conservata.

Il regolamento generale sulla protezione dei dati definisce inoltre le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati:[40]

- "una descrizione dei trattamenti previsti e delle finalità del trattamento";
- "una valutazione della necessità e proporzionalità dei trattamenti";
- "una valutazione dei rischi per i diritti e le libertà degli interessati";
- "le misure previste per:
  - "affrontare i rischi";
  - "dimostrare la conformità al presente regolamento".

Si ricorda inoltre che l'inosservanza degli obblighi concernenti la DPIA può comportare l'imposizione di **sanzioni pecuniarie** da parte delle Autorità garanti. Il mancato svolgimento dell'analisi, quando il trattamento è soggetto a tale valutazione possono comportare l'applicazione di una sanzione amministrativa fino ad un massimo di 10 milioni di euro e, se si tratta di un'impresa, fino al 2% del fatturato globale annuo.

4.4. Valutare se necessaria la consultazione preventiva dell'autorità di controllo

Una volta effettuata la valutazione di impatto sulla protezione dei dati il titolare del trattamento potrà decidere in autonomia se iniziare il trattamento, qualora ritenga di avere adottato tutte le misure idonee e sufficienti per mitigare il rischio. Il titolare del trattamento tuttavia, qualora ritenga all'esito della valutazione di impatto di **non essere in grado di trovare misure sufficienti per ridurre il rischio ad un livello accettabile** e per dimostrare la conformità rispetto al GDPR, dovrà consultare preventivamente l'autorità di vigilanza competente per ottenere indicazioni su come gestire il rischio residuale.[41]

---

39 Le Linee Guida prevedono infatti che "*L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità. Può essere altresì necessario ripetere singole fasi della valutazione man mano che il processo di sviluppo evolve, dato che la selezione di determinate misure tecniche od organizzative può influenzare la gravità o la probabilità dei rischi posti dal trattamento*", WP 248 rev.01, *cit.*, pag. 16.

40 Articolo 35, c. 7, e considerando 84 e 90 GDPR.

41 Così è previsto dall'art. 36 GDPR. Il comma 3 dell'articolo prevede inoltre cosa debba comunicare il titolare del trattamento all'autorità di controllo:
a*) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del*

L'autorità non avrà quindi il compito di autorizzare il trattamento, bensì quello di **indicare le misure ulteriori** eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive previste dall'art. 58 del GDPR, dall'ammonimento del titolare al **divieto** di procedere al trattamento.

Dovrà valutarsi di volta in volta quindi, in relazione al rischio residuo che il titolare del trattamento ritiene permanere all'esito dello svolgimento della valutazione di impatto, l'effettiva necessità di consultare l'autorità di controllo tenendo tuttavia presente che tutte le volte in cui ci si trovi nella condizione di dover gestire un rischio derivante da certi tipi di trattamento o dall'estensione e frequenza del trattamento, da cui potrebbe derivare altresì un danno o un'interferenza con i diritti e le libertà della persona fisica[42] è sempre prudente consultare preventivamente l'autorità. La controindicazione è che i tempi, se pur contingentati, sono piuttosto lunghi. Inoltre, non è previsto un sistema generale espresso di silenzio-assenso.[43]

In via ipotetica e generale si potrebbe quindi ritenere necessario che il titolare del trattamento si rivolga all'autorità per ottenere un parere preventivo nel caso in cui per esempio il trattamento che si prevede di effettuare implichi una profilazione molto alta dell'interessato, come potrebbe verificarsi nel caso in cui la finalità del trattamento sia l'elaborazione di un sistema di *raccomendation*, mentre potrebbe al contrario essere sufficiente l'aver svolto la sola valutazione di impatto senza la necessità di consultare l'autorità di controllo nel caso in cui scopo del trattamento sia quello di fornire all'interessato migliori indicazioni per la navigazione all'interno di una struttura.

Infine si tenga presente che come per la disciplina relativa alla DPIA, anche lo svolgimento non corretto o la mancata consultazione dell'Autorità di controllo competente ove ciò sia necessario può comportare l'applicazione di una sanzione amministrativa fino ad un massimo di 10 milioni di euro e, se si tratta di un'impresa, fino al 2% del fatturato globale annuo.

***

Resto a disposizione per ogni ulteriore chiarimento e integrazione, cogliendo l'occasione per porgere i miei più cordiali saluti.

Avv. Carlo Piana

---

trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
b) *le finalità e i mezzi del trattamento previsto;*
c) *le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;*
d) *ove applicabile, i dati di contatto del titolare della protezione dei dati; 4.5.2016 L 119/54 Gazzetta ufficiale dell'Unione europea IT*
e) *la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;*
f) *ogni altra informazione richiesta dall'autorità di controllo.*

42 Considerando 94 GDPR.

43 Sempre Considerando 94 GDPR