Dicembre 2020

Privacy by design e by default: come la protezione dei dati diventa elemento di sviluppo

Massimiliano Masnada e Giulia Mariuz, Hogan Lovells Studio Legale

Lo scorso 20 ottobre il Comitato Europeo per la protezione dei dati ha adottato in via definitiva le linee guida in materia di *data protection by design and by default* ("**Linee Guida**"). Le Linee guida trattano in maniera approfondita il concetto di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, di cui all'art. 25 del Regolamento 679/2016 ("**GDPR**").

Le Linee Guida si rivolgono principalmente ai titolari del trattamento, ossia a coloro che decidono le finalità e le modalità del trattamento dei dati personali nell'ambito delle diverse attività. Tuttavia, altri attori, come gli intermediari e i fornitori di prodotti, servizi e applicazioni, pur rivestendo nella maggior parte dei casi il ruolo di "responsabile" del trattamento e non essendo direttamente interessati dal citato art. 25 del GDPR, possono utilizzare le Linee Guida come *benchmark* di riferimento nella creazione di prodotti e servizi conformi al GDPR e quindi spendibili sul mercato con il "bollino di qualità" del rispetto della privacy.

La *privacy by design e by default* è una declinazione del principio di responsabilizzazione, o *accountability*, sul quale si fonda l'impianto normativo del GDPR. L'*accountability* prevede in particolare che le società titolari del trattamento siano in grado di dimostrare in ogni momento la corretta attuazione delle norme a tutela della protezione dei dati, nonché delle garanzie per i diritti e le libertà degli interessati, mediante l'adozione di misure tecniche e organizzative adeguate.

Il GDPR non specifica quali debbano essere queste misure, che secondo le Linee Guida possono essere "*anything*": dal ricorso alle tecnologie più avanzate, al *training* di base dei dipendenti, alla pseudonimizzazione, alla sottoscrizione di adeguate tutele contrattuali. Spetta al titolare valutare i presidi organizzativi e di sicurezza più adatti in concreto, tenendo conto di specifici parametri che l'art. 25 del GDPR individua nello stato dell'arte e nei costi di attuazione, nella natura dei dati trattati nonché nell'ambito di applicazione, nel contesto e nelle finalità del trattamento. L'approccio è quello basato sull'analisi del rischio per i diritti fondamentali e le libertà individuali insito al trattamento. Senza correre il rischio di un paragone ardito, si può dire che il titolare del

trattamento deve compiere un'analisi del rischio rispetto agli strumenti utilizzati per le operazioni di trattamento dei dati personali simile, per impostazione e valenza ontologica, a quello che effettua al fine dell'adozione delle misure di igiene e sicurezza sul lavoro imposto dal D..Lgs. 81/08.

Le Linee Guida chiariscono in primo luogo che i titolari devono considerare la protezione dei dati personali quale elemento imprescindibile di ciascun trattamento "sin dalla progettazione", ovvero dal "momento della determinazione delle modalità del trattamento". Si parla, in tal caso, di *privacy by design* in quanto la protezione dei dati influenza il processo di *decision making* e le scelte del titolare rispetto agli strumenti utilizzati per le operazioni di trattamento, o quantomeno contribuisce alle stesse nel senso di plasmarle, di modo che il trattamento sia – già nella sua fase embrionale, quindi fin dalla progettazione – predisposto a garantire i principi fondamentali del GDPR. Va da sé che, in base al principio di minimizzazione dei dati, di cui sicuramente la *privacy by design* può essere considerata un corollario, occorre avere riguardo sia ad una dimensione quantitativa dei dati personali raccolti, imponendone il trattamento esclusivamente nella misura indispensabile al conseguimento dello scopo perseguito, sia ad una dimensione qualitativa che consenta il raggiungimento dello scopo medesimo attivamente, privando il più possibile le informazioni personali del loro potere identificativo.

In questo senso, le Linee Guida sanciscono il definitivo tramonto dell'approccio "estetico" alla privacy dei consensi istituzionali che caratterizzava il panorama normativo pre-GDPR, conferendo invece alla protezione dei dati un ruolo chiave nei processi aziendali, con particolare riguardo alla scelta degli applicativi utilizzati, alla selezione dei fornitori e, più in generale, agli aspetti organizzativi a supporto dei trattamenti. Si può affermare, in un certo senso, che il diritto alla privacy perde un po' della sua natura dispositiva in capo all'interessato per assurgere, nella sua dimensione di *privacy by design*, ad un canone di ordine pubblico che prescinde dalla volontà del singolo, ma ricopre un requisito di *accountability* imposto dal GDPR a coloro che svolgono una attività sistematica di trattamento dei dati personali.

In maniera del tutto speculare, la protezione dei dati per impostazione predefinita comporta che il titolare effettui delle scelte ben precise, non solo nella scelta degli strumenti ma anche in relazione alle modalità dell'utilizzo degli stessi nel quadro delle attività di trattamento. Tali strumenti devono essere impostati, da un punto di vista strettamente tecnico, in modo da garantire il rispetto della minimizzazione dei dati e degli altri richiamati principi fondamentali del GDPR. Ciò significa, ad esempio, che gli applicativi devono essere settati in modo da evitare *by default*, appunto, la raccolta o la conservazione di dati ultronei alle finalità perseguite. Le Linee Guida specificano che, laddove il titolare utilizzi *software* terzi o soluzioni tecnologiche *off the shelf*, deve effettuare un vero e proprio *risk assessment* sul prodotto ed assicurarsi che le funzionalità incompatibili con le finalità del trattamento siano disattivate.

Per le ragioni esposte, come anticipato in premessa, le Linee Guida si rivolgono non solo ai titolari del trattamento ma anche ai produttori e fornitori di beni e servizi (che agiscono come responsabili del trattamento, cioè trattando dati per conto del titolare) quali ad esempio fornitori di servizi *cloud*, di soluzioni di *data analytics* o *strong authentication* per finalità antifrode. Come tali, essi sono *key player* nella corretta applicazione della *privacy by design* e *privacy by default*. Gli obblighi che insistono sui titolari del trattamento sono infatti in grado di condizionare la domanda di mercato rispetto ad applicativi e servizi che dovranno essere offerti dai produttori e dagli intermediari incorporando proprio l'elemento di protezione del dato quale *feature* essenziale del prodotto. Le Linee Guida sono molto chiare: quando i responsabili trattano dati per conto dei titolari, devono mettere al servizio di questi ultimi la loro esperienza per costruire la fiducia necessaria e accompagnare i propri clienti – incluse le PMI – nel processo di progettazione, fornendo soluzioni e applicativi in cui la protezione dei dati è *embedded*, incorporata. A contrario, ciò significa che la progettazione di tali prodotti e servizi deve facilitare le esigenze di compliance dei titolari i quali sono, in ultima analisi, responsabili per il rispetto del GDPR.

Le stesse considerazioni valgono in relazione alle misure organizzative a supporto delle attività di trattamento. In tal senso, si fa riferimento all'allocazione delle credenziali di autorizzazione all'accesso ai database, alla segregazione delle funzioni e degli accessi, alle istruzioni agli incaricati rispetto all'utilizzo corretto dei dati personali e allo svolgimento delle operazioni di trattamento, alla corretta formazione aziendale, ecc.

Definita così la portata dell'art. 25 del GDPR, le Linee Guida offrono una lettura concreta della *privacy by design* e *privacy by default* declinata nel contesto dei principi fondamentali del GDPR tra cui quello della trasparenza e legittimità del trattamento, di limitazione delle finalità del trattamento, di minimizzazione dei dati, della accuratezza e proporzionalità dei dati trattati nonché di quello di *data retention*. Rispetto a tali principi, le Linee Guida offrono esempi concreti che chiariscono la portata applicativa della *privacy by design* e *privacy by default* in ogni momento del trattamento, incluse le fasi di *procurement*, *outsourcing*, sviluppo, supporto, mantenimento, *testing*, conservazione, cancellazione, etc..

A titolo esemplificativo, di seguito alcuni degli esempi inclusi nelle Linee Guida per ciascuno dei principi fondamentali del GDPR.

Trasparenza

Il titolare del trattamento deve essere chiaro nei confronti dell'interessato fin dall'inizio in merito alla raccolta e all'utilizzo dei dati personali dello stesso. Il rispetto di questo principio implica, tra le altre cose, che le informazioni devono essere in un linguaggio chiaro e semplice, conciso e comprensibile; la comunicazione deve avere un chiaro significato per gli interessati; e le informazioni devono essere rese in modo facilmente accessibile. Questi principi vanno valutati anche in relazione all'ambiente e al tipo di trattamento effettuato.

Un titolare sta progettando come strutturare l'informativa privacy sul proprio sito web al fine di soddisfare i requisiti di trasparenza. L'informativa non dovrebbe contenere una mole di informazioni di difficile comprensione per gli interessati. Al contrario, deve essere scritta in un linguaggio chiaro e conciso in modo da facilitare gli utenti nella comprensione delle modalità di trattamento dei loro dati personali.

Il titolare decide dunque di fornire le informazioni necessarie in base ad un approccio *layered*, evidenziando i passaggi più importanti. Informazioni più dettagliate sono facilmente disponibili tramite menu a tendina e link a pagine di approfondimento.

Il titolare si assicura inoltre che le informazioni siano fornite tramite diversi canali, rendendo disponibili brevi video per illustrare in maniera *user friendly* i passaggi più rilevanti. La sinergia tra le varie pagine e i diversi canali di comunicazione è fondamentale per garantire che l'approccio illustrato non aumenti la confusione, ma piuttosto la riduca.

Infine, affinché gli interessati accedano in maniera semplice e veloce all'informativa, la stessa è resa disponibile tramite hyperlink bene in evidenza su tutte le pagine del sito web in questione.

Legittimità

La legittimità comporta che il titolare debba valutare in ogni momento la sussistenza di una base giuridica adeguata per ciascun trattamento.

Una banca sta valutando l'implementazione di un processo per migliorare l'efficienza nella gestione delle richieste di finanziamento. L'idea dietro il servizio è che la banca, richiedendo al cliente l'autorizzazione, raccolga i suoi dati direttamente dall'autorità fiscale.

La raccolta di dati personali in merito alla situazione finanziaria dell'interessato è necessaria per effettuare le valutazioni dovute, su richiesta dell'interessato, prima della concessione di un finanziamento. Tuttavia, la raccolta di dati personali direttamente dall'amministrazione fiscale non è necessaria, in quanto il cliente può fornire quegli stessi dati alla banca direttamente. Anche se

la banca può avere un interesse legittimo ad acquisire la documentazione direttamente dalle autorità fiscali, ad esempio per garantire l'efficienza nell'elaborazione dei prestiti, tale accesso diretto comporta un rischio legato a potenziali abusi.

Nell'attuare il principio di legittimità, la banca, quale titolare del trattamento, si rende conto che in questo contesto la raccolta diretta di dati dall'autorità fiscale non può basarsi sulla necessità contrattuale e valuta la sussistenza di altre basi giuridiche. Nel particolare Stato membro in cui si trova la banca, vi sono leggi nazionali che permettono alla banca di raccogliere informazioni direttamente dalle autorità fiscali pubbliche, se l'interessato vi acconsente preventivamente.

La banca presenta quindi le informazioni relative al trattamento in oggetto sulla piattaforma di richiesta online in modo tale da facilitare agli interessati la comprensione degli aspetti obbligatori del trattamento e di quelli non necessari. Le modalità del trattamento, per impostazione predefinita, non consentono la raccolta dei dati da titolari terzi e la possibilità di fornire direttamente i dati è presentata in modo da non dissuadere l'interessato. L'eventuale consenso alla raccolta diretta dei dati presso titolari terzi è limitato ad un accesso temporaneo a un insieme specifico di informazioni. L'eventuale consenso è trattato elettronicamente in modo documentabile e agli interessati è resa disponibile la possibilità di verificare in ogni momento le proprie scelte e di revocare il consenso prestato.

La banca, in qualità di titolare, ha valutato in anticipo questi requisiti di *privacy by design e by default* e li include espressamente nel capitolato della gara d'appalto per l'acquisto della piattaforma. Il titolare è consapevole che, non includendo tali requisiti nella gara d'appalto, corre il rischio di subire ritardi o dover sostenere costi molto alti al momento dell'implementazione della soluzione al fine di garantire il rispetto della normativa.

Correttezza

Il principio di correttezza richiede che i dati personali non vengano trattati in modo dannoso, discriminatorio, imprevisto o fuorviante per l'interessato.

Un titolare del trattamento tratta i dati degli utenti nell'ambito della fornitura di un servizio di streaming in cui gli utenti possono scegliere tra un abbonamento "standard" e un abbonamento "premium" in cui lo streaming è di migliore qualità.

Nell'ambito dell'abbonamento "premium", agli abbonati viene data priorità da parte del servizio clienti.

In base al principio di correttezza, tale priorità non può discriminare l'accesso da parte degli abbonati al servizio "standard" all'esercizio dei loro diritti in base al GDPR.

Ciò significa che, sebbene agli abbonati "premium" venga data priorità al servizio, il riscontro alle richieste degli abbonati al servizio "standard" dovrà avvenire senza indebito ritardo, e comunque nel rispetto delle tempistiche massime previste dalla normativa.

Limitazione delle finalità

In base a tale principio il titolare del trattamento deve raccogliere dati per finalità specifiche, esplicite e legittime, e non trattarli ulteriormente in modo incompatibile con le finalità per le quali sono stati originariamente raccolti.

Un titolare del trattamento tratta dati dei propri clienti al fine di adempiere al contratto in essere, cioè per consegnare la merce all'indirizzo corretto e ottenere il pagamento. I dati personali memorizzati sono la cronologia degli acquisti, il nome, l'indirizzo, l'indirizzo e-mail e il numero di telefono.

Il titolare sta valutando l'acquisto di un prodotto di Customer Relationship Management (CRM) che raccoglie in maniera unitaria tutti i dati sulle vendite, il marketing e il servizio clienti. Il prodotto fornisce la possibilità di memorizzare tutte le telefonate, le attività, i documenti, le e-mail e le campagne di marketing per ottenere una ricostruzione a 360 gradi del cliente. Inoltre, il CRM è in grado di analizzare automaticamente il potere d'acquisto dei clienti utilizzando informazioni pubbliche. Lo scopo dell'analisi è quello di migliorare l'attività di marketing personalizzata.

Tali attività non rientrano nelle finalità originarie legittime del trattamento. Per essere in linea con il principio della limitazione delle finalità, il titolare richiede al fornitore del prodotto di effettuare un'attività di mappatura delle diverse attività di trattamento nell'ambito delle finalità rilevanti per il titolare. Dopo aver ricevuto i risultati della mappatura, il titolare valuta se la finalità di marketing e quella della pubblicità mirata sono compatibili con le finalità originarie e se sussistano delle basi giuridiche adeguate. In caso negativo, il titolare rinuncia ad utilizzare le funzionalità del prodotto. In alternativa, il titolare potrebbe scegliere di rinunciare alla mappatura e successiva valutazione e semplicemente astenersi dall'utilizzare le funzionalità descritte.

Minimizzazione dei dati

Tale principio implica che debbano essere elaborati solo i dati personali adeguati, pertinenti e limitati a quanto necessario alla finalità perseguita. I dati dovrebbero essere trattati quanto più possibile in forma anonima o pseudonimizzata.

Un corriere mira a valutare l'efficacia delle sue consegne in termini di tempi di consegna, carico di lavoro, programmazione e consumo di carburante. Per raggiungere questo obiettivo, il corriere deve elaborare una serie di dati personali relativi sia ai dipendenti (autisti) che ai clienti (indirizzi, articoli da consegnare, ecc.) Questa operazione di trattamento comporta rischi sia per il monitoraggio dei dipendenti, che richiede specifiche tutele legali, e il monitoraggio delle abitudini dei clienti attraverso la conoscenza degli articoli consegnati oltre tempo. Questi rischi possono essere notevolmente ridotti con un'adeguata pseudonimizzazione dei dati dei dipendenti e dei clienti. In particolare, se le chiavi di pseudonimizzazione sono spesso alternate, e vengono prese a riferimento macro aree invece di indirizzi puntuali, si persegue un'efficace minimizzazione dei dati e il titolare può concentrarsi esclusivamente sul processo di consegna e sull'attività di ottimizzazione delle risorse, senza incrociare la soglia di monitoraggio dei comportamenti dei singoli (clienti o dipendenti).

Accuratezza

I dati personali devono essere precisi e aggiornati e devono essere adottate tutte le misure necessarie a garantire che i dati personali inesatti, tenendo conto delle finalità per le quali vengono trattati, siano cancellati o rettificati.

Una società assicurativa desidera utilizzare l'intelligenza artificiale (IA) per effettuare attività di profilazione dei propri clienti come base per calcolare il rischio di polizza. Nel determinare come la soluzione di IA dovrebbe essere sviluppata e nel valutare le offerte dei fornitori, la società deve tenere in considerazione la *privacy by design*. Nel valutare come impostare la IA, il titolare dovrebbe utilizzare dati accurati per garantire che IA funzioni in maniera precisa.

La società assicurativa seleziona pertanto un campione di clienti rappresentativo dell'intera base clienti al fine di evitare forme di discriminazione. I dati sono dunque raccolti dai rispettivi sistemi di trattamento e includono informazioni in merito al tipo di assicurazione, così come dati da registri pubblici a cui la società ha legittimamente accesso. Tutti i dati sono sottoposti a pseudonimizzazione prima di essere trasferiti al sistema dedicato al *training* del modello di IA. Per garantire che i dati utilizzati nell'ambito dell'attività di *training* della IA siano quanto più accurati possibile, il titolare raccoglie dati esclusivamente da fonti contenenti informazioni corrette e aggiornate. La società assicurativa effettua dei test per garantire che IA sia affidabile e fornisca dei risultati non discriminatori sia nel corso dello sviluppo che prima che il prodotto sia rilasciato. Al termine dell'attività di *training* di IA, la società assicurativa si serve dei risultati restituiti nell'ambito di valutazione e determinazione del rischio, ma astenendosi dall'affidarsi unicamente ai risultati di IA salvo tale trattamento automatizzato sia legittimo ai sensi del GDPR. La società assicurativa effettuerà anche revisioni periodiche dei risultati restituiti da IA, al fine di mantenerne l'affidabilità e, ove necessario, apportare modifiche all'algoritmo.

Limitazione della conservazione

Secondo tale principio, i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Il titolare raccoglie dati personali al fine di gestire una *membership* dell'interessato. I dati dovrebbero essere cancellati quando il soggetto cessa di appartenere a quell'associazione o organizzazione e non sussistono ulteriori basi giuridiche per conservare i dati. Il titolare prepara una procedura interna sulla *retention* del dato, in base alla quale i dipendenti devono cancellare manualmente i dati personali al termine del periodo di conservazione. Il dipendente si attiene a tale procedura, ma per rendere la cancellazione ancora più efficace (e minimizzare il rischio di errori), il titolare implementa un sistema di cancellazione automatica. Il sistema è configurato in modo da garantire la cancellazione periodica a intervalli predefiniti di tutti i dati personali da tutti gli applicativi della società. Il titolare rivede ed effettua dei *test* periodici sulla procedura di *retention*.

Sicurezza e integrità

I dati devono essere protetti da adeguate misure di sicurezza al fine di tutelarli, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Un titolare vuole estrarre grandi quantità di dati personali da un database medico che contiene informazioni sanitarie ad un database dedicato della società a fini di controllo qualità.

La società ha effettuato una valutazione del rischio in merito al trasferimento degli estratti rilevanti ad un server accessibile a tutti i dipendenti della società ed ha individuato un alto rischio. Dal momento che solo un dipartimento della società ha la necessità di trattare i dati, il titolare decide di limitare l'accesso al server dedicato ai dipendenti di quel dipartimento.

In aggiunta, per limitare ulteriormente il rischio, i dati saranno pseudonimizzati prima di essere trasferiti. Per regolamentare l'accesso e mitigare possibili danni derivanti dal *malware*, la società decide di segregare il *network*, e stabilire controlli d'accesso al server. In aggiunta, stabilisce procedure di controllo della sicurezza e un sistema di prevenzione e individuazione di accessi indebiti. Viene inoltre implementato un sistema di auditing al fine di monitorare gli accessi e le modifiche che genera report e alert automatici al verificarsi di determinati eventi pre-configurati. Il titolare si assicura inoltre che gli utenti abbiano accesso su base *need to know* e con i livelli d'accesso adeguati.

In questo modo, utilizzi indebiti possono essere velocemente individuati.

A ben vedere, scorrendo gli esempi proposti dal Comitato europeo per la protezione dei dati, emerge come la protezione dei dati sin dalla progettazione e per impostazione predefinita non sia altro che il *trade d'union* che permette ai titolari di applicare efficacemente i principi fondamentali del GDPR sopra citati, ovvero in modo da essere in grado di dimostrare in ogni momento di aver agito in questo senso. Tramite la *privacy by design e by default*, la protezione dei dati entra nei processi aziendali quale formidabile elemento di sintesi tra la tecnologia e il diritto, le procedure operative e le norme di compliance. Alla luce delle Linee Guida, è evidente che l'applicazione tempestiva di questi principi risulta di fondamentale importanza nella tutela effettiva dei diritti e delle libertà degli interessati, e nella corretta applicazione dei requisiti del GDPR. Da questo punto di vista, la protezione dei dati fin dalla progettazione e per impostazione predefinita rappresenta un elemento di sviluppo fondamentale tramite il quale le aziende hanno la possibilità di convertire i potenziali costi derivanti dalla compliance in un enorme vantaggio competitivo.