L’accountability oltre il registro dei trattamenti

L’accountability (ovvero il principio di responsabilizzazione nella terminologia adottata nella traduzione italiana del Regolamento generale sulla protezione dei dati) è, probabilmente, l’innovazione maggiore che la norma europea ha apportato nell’ambito della protezione dei dati personali per il nostro Paese.

Il principio di responsabilizzazione, infatti, sposta il timone della protezione dei dati dalle mani del Garante a quelle del titolare del trattamento (e in certa parte, del responsabile del trattamento, inteso come soggetto terzo rispetto all’organizzazione del titolare) imponendogli non solo di garantire il rispetto dei principi che presiedono al trattamento dei dati, ma anche di comprovare il suo operato: il regolamento, spesso, si limita a fissare i parametri entro i quali dovranno prendere forma le scelte del titolare, e solo in pochi casi pone direttamente gli adempimenti ai quali il titolare dovrà attenersi.

Quindi, da una parte, si lascia al titolare un certo margine di scelta: è chiaro che il principio di accountability va letto in armonia con l’approccio basato sul rischio, che non prescinde dal contesto in cui opera il titolare; imprese di dimensioni diverse, che operano trattamenti diversi, non saranno costrette a prendere le stesse misure di protezione (sia che si tratti di misure di sicurezza, sia che si tratti di misure organizzative). D’altra parte consente al titolare anche, per così dire, di precostituire le prove che saranno destinate a comprovare il suo diligente operato, e la congruità delle scelte effettuate. Si tratta di un vantaggio non da poco, che però, per essere colto appieno necessita di un radicale cambio di mentalità: non ci saranno adempimenti da burocratizzare al solo scopo di evitare sanzioni, ma occorre

operare proattivamente scelte congrue e bilanciate, e imparare a comprovarle.

Insomma, una volta tanto, bisogna abbandonare la strada vecchia per la nuova, azione che sappiamo tutti essere sconsigliata dal vecchio adagio popolare e che probabilmente è endemicamente vissuta come incauta dal nostro subconscio sociale, tanto che anche il legislatore nazionale è stato indotto, nel tentativo di mantenere il più possibile in vita il vecchio impianto ben più familiare, a discutibili interventi mirati a riportare la misura della discrezionalità nelle mani dell'Autorità (mi riferisco, in particolare al tentativo di azzerare la valutazione del titolare in tema di legittimo interesse, o alla pervicace riproposizione dei ruoli interni).

E' fondamentale, però, in un sistema fondato sull'accountability, non scambiare la documentabilità delle scelte operate con un onere di burocratizzazione che si risolve in una inutile proliferazione di scartoffie (in senso lato, anche digitali quindi).

Cosa occorrerà documentare dunque?

Il registro dei trattamenti

Quando si parla di accountability si pensa subito ai registri delle attività di trattamento, probabilmente anche in ragione di una certa somiglianza che pare avere, di primo acchito, con il documento programmatico sulla sicurezza, croce e delizia (a seconda dell'approccio più o meno passivo) dei titolari italiani fino al 2011.

Sarebbe però un errore appiattire l'accountability solo sul registro: e ancora più da evitare sarebbe l'errore di appiattire la funzione del registro a mero onere compilativo, come molti fecero al tempo del DPS: esattamente come avveniva per il DPS, il registro delle attività di trattamento ha il

compito di fotografare i trattamenti operati, in modo da costituire un ausilio e non un intralcio alle attività di monitoraggio o controllo che deve operare il titolare (o chi per lui).

Il contenuto tassativo del registro delle attività di trattamento è contenuto nell'articolo 30 del regolamento generale sulla protezione dei dati, e molte autorità nazionali hanno pensato di fornire modelli per aiutare titolari e responsabili nella sua tenuta: i più noti, probabilmente sono quelli forniti dalla CNIL e dall'autorità belga.

Anche l'ICO, l'autorità che presiede alla protezione dei dati nel Regno Unito, ha fornito un suo modello; chi scrive lo ha trovato oltremodo interessante, e nel prosieguo si tenterà di fornire alcuni elementi suggeriti nel modello che, probabilmente, meritano attenzione anche in Italia.

Anche perché, se abbiamo difficoltà anche solo a tradurla l'accountability, forse è meglio trarre ispirazione da chi, invece, questo istituto lo conosce bene.

L'ICO fornisce due versioni del registro: una per il titolare e una per il responsabile. Quella del responsabile, da utilizzare per i trattamenti che egli effettua per conto di altri è molto snella, adatta per chi deve tenere traccia di una molteplicità di trattamenti effettuati per altrettanti clienti. E' importante sottolineare che, qualora si volesse impiegare il modello fornito da un'autorità straniera, questo andrebbe tradotto in italiano prima di essere impiegato. Le autorità che procederanno al controllo, infatti, opereranno nella nostra lingua e non è consigliabile mantenere i modelli in lingua straniera, anche se poi venissero compilati in italiano: così come è sconsigliabile usare termini stranieri nella documentazione o nelle comunicazioni ufficiali: ad esempio, sarà bene non individuare il responsabile della protezione dei dati con l'acronimo DPO o con il corrispondente "data protection officer" anche se, per comodità e per non

ingenerare confusione con altri termini simili o anche solo per abitudine, a volte, informalmente, si preferisce optare per la definizione anglofona (la traduzione del RGPD non è delle più felici, il lettore italiano deve destreggiarsi tra responsabilità, responsabilizzazione, responsabile del trattamento e responsabile della protezione, rispetto a termini come accountability, liability, processor e data protection officer che risultano, dal punto di vista linguistico, marcatamente distanti).

Tornando ai modelli di registro forniti dall'ICO, la struttura suggerita per il titolare è più complessa e si compone di due parti: una parte obbligatoria, e una facoltativa, dettata da ragioni di opportunità, proprio in ragione del controllo sui trattamenti che il registro dovrebbe garantire ai titolari.

Inoltre l'ICO distingue le annotazioni che occorre effettuare in ottemperanza al regolamento europeo da quelle che occorre effettuare per adempiere alla sua normativa nazionale (ovvero il Data Protection Act, che, comunque potrebbe essere foriero di qualche spunto anche per l'Italia, come si vedrà nel prosieguo).

In ogni sezione l'ICO indica l'adempimento che pone alla base dell'onere di documentazione e consiglia di utilizzare documenti elettronici in modo che sia possibile collegarli tra loro e aggiornarli con facilità. E' chiaro, che si tratta di un ottimo consiglio, ma qui, per gli italiani, si innesta anche la normativa sulla conservazione digitale dei documenti, e quindi, ove si tratti di documenti informatici che debbono essere conservati a norma anche per altri fini (penso, ad esempio ai contratti e agli accordi sul trattamento) sarà bene domandarsi se non occorra anche valutare l'adozione di un sistema di conservazione. Chiaramente analogo problema si pone anche per la valida sottoscrizione degli accordi in forma digitale.

Ove non si disponesse di strumenti che consentano di

sottoscrivere validamente gli accordi (ad esempio) e di conservarli digitalmente nel tempo, i campi del registro in cui l'ICO indichi che vanno linkati i relativi documenti potranno essere compilati indicando semplicemente ove quel documento sia stato archiviato (e si potrà anche eventualmente digitalizzarne una mera copia, per comodità).

Già da quanto detto sin qui si comprende che sebbene l'ICO ponga il registro al centro della documentazione da predisporre al fine di dimostrare la propria conformità alla normativa, egli non lo considera affatto l'unico documento richiesto ai fini dell'accountability, anzi.

L'informativa come linea guida per l'accountability

Ai titolari che si domandino quali adempimenti vadano documentati, l'ICO risponde di guardare l'informativa (che è essa stessa rilevante al fine di dimostrare la conformità al GDPR): infatti, mutando la prospettiva, nell'informativa il titolare dà atto di molte delle scelte che ha operato e che vanno, appunto comprovate, ossia "documentate".

Ad esempio: l'informativa impone di evidenziare agli interessati la base giuridica dei trattamenti; per i trattamenti basati sul legittimo interesse potrebbe essere opportuno[1] anche dare atto, sinteticamente, del bilanciamento operato e del perché di è ritenuto prevalente l'interesse del titolare.

Tale sintetica indicazione dovrà essere corredata da una valutazione scritta (che non viene inserita nell'informativa), che lasci agli atti e renda palese, in caso di controlli o di istanze, il bilanciamento degli interessi operato dal titolare. Quindi: l'annotazione sintetica che si dà nell'informativa non esaurisce gli obblighi ai quali è tenuto il titolare in ottemperanza al principio di

responsabilizzazione.

Muovendo dall'informativa, quindi, e dagli elementi che dovrà fornire agli interessati e dei quali e bene, quindi, che tenga traccia de:

- la **base giuridica** dei trattamenti;
- il **legittimo interesse** (e il bilanciamento operato[2]);
- i correlati **diritti dell'interessato** (non sempre l'interessato gode di tutti i diritti: ad esempio, la portabilità dei dati è un diritto riconosciuto solo in caso di trattamenti basati su consenso o contratto; sarà bene che i diritti dell'interessato siano specificati a seconda della base giuridica su cui poggia il trattamento). E' bene predisporre documentazione che agevoli l'esercizio dei diritti dell'interessato e procedure interne per poter tempestivamente fornirgli riscontro.
- L'**esistenza di decisioni automatizzate**, inclusa la profilazione;
- la **fonte dei dati personali** (le informazioni da dare agli interessati (e i tempi in cui darle) variano, infatti, a seconda che i dati siano stati raccolti presso l'interessato stesso o presso terzi e in questo secondo caso deve essere informato della fonte di raccolta) .

Una volta che il titolare abbia fissato questi aspetti, egli potrà procedere a predisporre ulteriore documentazione,che può evincersi dagli adempimenti che il Regolamento impone al titolare in ordine a:

- **registrazione dei consensi** (si dovrà infatti poter provare, per i trattamenti basati sul consenso, che il consenso è stato validamente acquisito)
- **accordi sul trattamento** (tra contitolari, ma anche tra titolare e responsabile del trattamento)
- **"dove" i dati sono trattati** (non in riferimento a

trasferimenti in Paesi terzi -elemento che è comunque richiesto dall'articolo 30 del GDPR -ma in riferimento ai sistemi informatici in cui sono trattati, ad esempio gestionali interni, servizi cloud, ecc: questo aspetto è fondamentale per garantire agli interessati l'esercizio dei loro diritti, ma anche per poter creare delle policy interne che consentano di autorizzare dipendenti e collaboratori in ordine ai diversi profili di trattamento)

- documentazione relativa a **violazioni di dati** (che impone non solo di dotarsi di efficaci procedure interne e modulistica per poter far fronte tempestivamente agli obblighi di comunicazione eventualmente previsti, ma anche di conservare la documentazione relativa alle violazioni subite, a prescindere dal fatto che la comunicazione sia stata effettuata o meno).
- **valutazione di impatto** sulla protezione dei dati: quando necessaria l'ICO consiglia non solo di tener traccia della DPIA effettuata, ma anche di tener traccia del suo stato di progressione, mentre la si effettua.

Alcuni di questi oneri "documentali" (che come si vede possono avere la forma più varia, spesso sostanziandosi in policy interne) sono imposti direttamente dal GDPR, altri invece sono opportuni per consentire al titolare un monitoraggio più efficace. Ad esempio, tenere traccia di "dove" i dati sono trattati potrebbe aiutare il titolare ad individuare trasferimenti all'estero dei quali non si è reso conto (operati magari inconsapevolmente attraverso l'uso di un sistema cloud), e incrociare tutte queste informazioni può ridurre la possibilità di omissioni o dimenticanze in ordine all'individuazione dei responsabili del trattamento; infine, una documentazione puntuale dei trattamenti ha indubbio vantaggio nella gestione delle istanze provenienti dagli interessati.

Non solo: la documentazione predisposta dal titolare,

accompagnata ad **audit e revisione** delle procedure interne e della contrattualistica può aiutare il titolare a monitorare la corretta applicazione della normativa.

E’ ovvio che il modello di registro dell’ICO dedica anche spazio alla sintetica indicazione delle **misure di sicurezza adottate**, in modo che sia sempre facile procedere a revisione a seconda del trattamento operato, ma si tratta di uno degli elementi imposti dall’articolo 30 del Regolamento: mi permetto di aggiungere che tener traccia anche della valutazione operata al momento della scelta e dell’adozione delle misure, potrebbe aiutare il titolare a rivedere più rapidamente, anche a distanza di tempo, se la valutazione può ancora considerarsi congrua, e potrebbe facilitarlo in caso di controlli. Mi permetto anche di aggiungere di non dimenticare le “misure di sicurezza” contrattuali: vincolare dipendenti e collaboratori ad un **accordo di riservatezza** destinato a perdurare anche oltre la cessazione del rapporto di lavoro o collaborazione è una misura ben più efficace della “nomina a incaricato” alla quale eravamo abituati, e può permettere, per certi versi, di raccordare la tutela dei dati personali con quella accordata alle informazioni commerciali (cfr. Trade Secret Directive).

Data retention policy

L’ICO, in applicazione della propria normativa interna, suggerisce anche di documentare le **politiche aziendali sulla conservazione e sulla cancellazione dei dati**: sebbene tali procedure non siano imposte dal GDPR è chiara l’utilità che possono avere per dimostrare la conformità del titolare al Regolamento, soprattutto in riferimento ad adempimenti, quali la cancellazione, che, in mancanza, sarebbero piuttosto difficili da provare.

L’intervento del WP29

L’ICO ricorda come il WP29 voglia alleggerire gli oneri documentali delle piccole e medie imprese, che quindi

potrebbero, in futuro, ricevere qualche “sconto”: tuttavia il WP29 non ha ancora provveduto sul punto (e peraltro se è vero che la documentazione aiuta a dimostrare la compliance al GDPR forse, anche in caso di “sconti,” sarà bene valutare cosa conviene comunque conservare).

Ci si permette di notare, tuttavia, che sino ad oggi il WP29 in realtà ha aggiunto più che togliere: ad esempio, in tema di data protection officer ha suggerito ai titolari e ai responsabili che versassero in stato di incertezza in ordine all’obbligo di designare il DPO, di procedere a una congrua **valutazione scritta** ove ritenessero di non dover procedere alla designazione, in modo da lasciarla a disposizione dell’autorità competente in caso di futuri controlli: e ciò proprio in ragione del principio di responsabilizzazione.

Sempre in tema di Data protection officer il WP29 ha consigliato di creare policy interne volte a precisare:

- tempistiche e modalità di coinvolgimento del DPO nelle decisioni riguardanti la protezione dei dati;
- determinazione più precisa delle ipotesi di conflitto di interesse;
- determinazione delle modalità e tempistiche di intervento del DPO nelle valutazioni di impatto sulla protezione dei dati

Non solo: è evidente come anche la **contrattualistica** con il data protection officer consentirà di valutare l’efficacia della sua azione, anche i termini di autonomia e indipendenza, e come anche questa vada ad aggiungersi alle misure di accountability.

Conclusioni

E’ chiaro che la “documentazione” delle attività descritta sin qui è parte dell’accountability, ma non la esaurisce: restano esclusi da questa breve disamina, ad esempio, i principi di

privacy by design e by default, le indicazioni in ordine al contenuto della contrattualista che aiuta il titolare a mantenere il controllo sui dati personali in outsourcing, o a regolare i suoi rapporti con il data protection officer, o sulla metodologia con cui condurre una DPIA, o ancora, i criteri con i quali procedere alla valutazione del bilanciamento degli interessi in caso di trattamenti basati su di esso (banalmente: se verrà meno – come chi scrive ritiene probabile- il provvedimento generale del Garante privacy in tema di videosorveglianza, occorrerà che ogni titolare proceda da sè al bilanciamento che il Garante aveva operato nel provvedimento generale dell'8 aprile 2010, sulla base del legittimo interesse).

Qui ci si è limitati, sulla scorta dei suggerimenti dell'ICO a individuare la documentabilità di scelte, compiute dal titolare, che potrebbe non apparire immediata, o a suggerire di integrare la documentazione obbligatoria con elementi che possono essere utili al titolare e che non gli sono, magari, immediatamente percepibili.

L'ICO a titolo esemplificativo consiglia inoltre, in estrema sintesi ai titolari e ai responsabili di munirsi (secondo le rispettive necessità) di politiche interne sulla riservatezza dei dati, sulla protezione dei dati, sulla sicurezza, sull'utilizzo dei sistemi (e qui, per noi, si aprirebbe anche tutto un capitolo in ordine all'utilizzo di sistemi aziendali, BYOD e controllo del lavoratore), sulla conservazione e sugli accordi di contitolarità e di accordi sul trattamento con i responsabili del trattamento.

L'ICO rammenta come documentare le attività di trattamento sia importante non solo perché è richiesto dalla normativa, ma anche perché è utile al titolare nella gestione dei dati e può aiutarlo a dimostrare la conformità ad altri aspetti del GDPR: insomma, la documentazione non ha valore in sé e per sé, come onere burocratico per scongiurare la sanzione, ma ha valore perché è di concreto ausilio al titolare nella sua attività di

gestione dei dati e controllo sulla correttezza dei trattamenti, e perché lo aiuta a dimostrare la compliance agli obiettivi fissati dal GDPR.

Si tratta di un approccio, ad avviso di chi scrive, molto simile a quello già efficacemente descritto su queste pagine, ma guardato dalla prospettiva dell'accountability.

A dimostrazione che i vari obblighi che discendono dal GDPR, ove gestiti con accortezza, non sono destinati a sovrapporsi, ma ad integrarsi tra loro, e ad integrarsi con la gestione aziendale in misura maggiore e probabilmente più efficace di quanto avvenisse con la precedente normativa nazionale, specie ove ci si fosse rassegnati supinamente a un approccio smaccatamente burocratico e non aderente alla realtà nella quale si fosse preteso di calarlo.

Note

1. Si vedano in proposito le linee guida (non ancora definitive) del Gruppo di lavoro articolo 29 in tema di trasparenza, ove è consigliato come buona pratica l'inserimento nelle informative di un sintetico accenno al bilanciamento operato: [adopted, but still to be finalized] Guidelines on Transparency under Regulation 2016/679 (wp260);
2. Per agevolare i titolari nel bilanciamento degli interessi l'ICO ha recentemente pubblicato anche un modello di valutazione in formato word ("sample LIA template") e una guida dettagliata (tutto in lingua inglese) reperibili all'indirizzo https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/

Bibliografia

A cura di: **Cesare Gallotti**

Lavora dal 1999 nel campo della sicurezza delle informazioni, della qualità e della gestione dei servizi IT.

Ha condotto progetti di consulenza per la pubblica amministrazione e per il settore privato. Opera, sia in Italia che all'estero, come Lead Auditor ISO/IEC 27001, ISO 9001, ISO/IEC 200000 e ISO 22301. Ha progettato ed erogato corsi di Quality Assurance e di certificazione Lead Auditor ISO/IEC 27001 e ITIL Foundation.

Tra gli attestati si segnalano: le certificazioni AICQ SICEV Lead Auditor ISO/IEC 27001, IRCA Lead Auditor 9001, CISA, ITIL Expert e CBCI, la qualifica come Lead Auditor ISO/IEC 20000 e il perfezionamento postlaurea in "Computer Forensics e investigazioni digitali".

E' capodelegazione del WG1 del comitato italiano ISO/IEC SC27 in UNINFO.

Ha pubblicato il libro, aggiornato nel 2017, "Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione; la norma ISO/IEC 27001:2013".

Cura la pubblicazione, dal 2008, della newsletter "IT Service management news" (http://www.cesaregallotti.it/Newsletter.html).

Web: www.cesaregallotti.it; Blog: blog.cesaregallotti.it

https://www.ictsecuritymagazine.com/articoli/laccountability-oltre-il-registro-dei-trattamenti/