Cristina Vicarelli
Avvocato

Regolamento generale sulla protezione dei dati: 13 cose da fare ora

Si parla molto dell'entrata in vigore del Regolamento generale sulla protezione dei dati (REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE), dopo la sua pubblicazione e di come la data del 25 maggio 2018, termine fissato per la sua piena applicazione, che costituisce un limite anche per l'adeguamento di titolari e responsabili (per i quali sono previste autonome sanzioni), non sia poi così lontana. Il Regolamento generale sulla protezione dei dati, però, seppure è una norma di applicazione diretta, non può essere calato *d'emblée* in una struttura aziendale. Occorreranno norme primarie, nazionali, non solo per armonizzarlo con la disciplina previgente che va ad abrogare -si pensi al Codice Privacy, dal quale si dovranno scorporare tutte le norme che non siano emanazione diretta della Direttiva 95/46/CE (norme mutuate dallo Statuto dei Lavoratori o dalla Direttiva E-privacy, ad esempio, che restano valide ed efficaci se non afferenti materie intaccate dalla novella di matrice europea)- ma anche per integrarlo, dato che i richiami alle normative nazionali sono presenti in maniera più o meno marcatamente derogatoria in una trentina di articoli.

A titolo meramente esemplificativo si pensi all'Articolo 88 del Regolamento generale sulla protezione dei dati, "Trattamento dei dati nell'ambito dei rapporti di lavoro" che lascia ampia discrezionalità agli Stati, oppure all'Articolo 85 "Trattamento e libertà d'espressione e di informazione" dove il bilanciamento tra libertà di espressione e protezione dei dati, tradizionalmente uno dei più delicati e problematici, è regolato in maniera assolutamente flessibile e generica, o ancora al richiamo alla conformità alla normativa interna degli Stati membri operata dall'Articolo 86 "Trattamento e accesso del pubblico ai documenti ufficiali" o le

ampie deroghe su base nazionale previste per trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici stabilite dall'Articolo 89.

Il richiamo alla normativa interna pertanto opera su due fronti: da un lato pone un'esigenza di integrazione e completamento della normativa europea, dall'altro mitiga l'esigenza di uniformità che ha mosso il legislatore europeo all'emanazione del Regolamento.

Non solo: vi sono anche aspetti pratici che attendono di essere perfezionati prima di poter essere implementati. Si pensi, sempre a titolo di esempio, alla possibilità di fornire informazioni in combinazione con icone standardizzate per dare, in modo facilmente visibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Sarà la Commissione a dover stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate: i titolari non possono improvvisare già da ora seguendo il loro estro.

Ma se il quadro normativo non è ancora completo e chiaro e mancano parecchi "pezzi" al puzzle, cosa possono fare titolari e responsabili per agire tempestivamente e non farsi trovare impreparati quando il Regolamento generale per la protezione dei dati sarà pienamente applicabile tra un paio d'anni?

Iniziare ad adeguarsi al Regolamento generale sulla protezione dei dati con i 12 step dell'ICO

Nella pratica non è facile, tuttavia l'ICO (che è l'Autorità per la protezione dei dati del Regno Unito) ha provato a stilare un decalogo, che si focalizza su 12 step che possono aiutare le imprese in questa primissima fase di adeguamento.

Io ho provato a leggere questi suggerimenti trasponendoli nel nostro ordinamento, in modo da evidenziarne eventuali peculiarità e la posizione di vantaggio da cui spesso partono i titolari italiani, dato che la nostra normativa è una di quelle che hanno applicato la Direttiva 95/46/CE in maniera più rigorosa. Non ho riportato fedelmente quanto detto dall'ICO, si tratta più che altro di un adattamento commentato. Consiglio pertanto la lettura del testo linkato in incipit a chi volesse conoscere l'esatto contenuto del decalogo originario.

L'ICO muove evidenziando come i principi e le principali definizioni della nuova normativa siano gli stessi della precedente, pertanto la maggior parte degli adempimenti resteranno validi: non si

tratta di un salto nel buio. Anzi, l'attuale approccio può rappresentare un buon punto di partenza sul quale costruire la futura compliance, tenendo a mente che, tuttavia, vi sono anche delle importanti novità, quindi bisognerà confrontarsi con nuovi adempimenti, da porre in essere per la prima volta, mentre alcuni di quelli noti dovranno essere modificati e adeguati.

Il decalogo predisposto dall'ICO si propone di essere utile proprio per evidenziare le differenze salienti tra la normativa attuale e il Regolamento generale sulla protezione dei dati, si tratta di un primissimo passo, dato che sia il Gruppo di Lavoro ex art 29, sia le autorità nazionali, anche in collaborazione tra loro, provvederanno nel prossimo biennio a dare linee guida in ordine alla applicazione del Regolamento, per quanto di competenza. Ai titolari e ai responsabili si consiglia di seguire attentamente gli sviluppi e le indicazioni che proverranno dagli organismi nazionali e da quelli europei.

L'ICO sottolinea la necessità che i titolari e i responsabili comincino a pianificare l'adeguamento alla nuova normativa quanto prima, anche per la necessità di coinvolgere le persone chiave della propria organizzazione ove fosse opportuno prevedere nuove procedure interne, garantire più trasparenza per i trattamenti, assicurare maggiori diritti o garantirne di nuovi. Teniamo presente che il corpus normativo del Regolamento è triplicato rispetto a quello della Direttiva che va a sostituire. Si tratta di intraprendere azioni che per le le imprese e gli enti più grandi e complessi potrebbero richiedere tempi lunghi e impegni di spesa, implicando interventi sul comparto IT, sul personale (anche rivolgendosi a professionalità attualmente non presenti in organigramma), sulla governance e sulle comunicazioni.

Il Regolamento generale sulla protezione dei dati introduce un termine che nella traduzione ufficiale è stato reso con "responsabilizzazione": l'accountability.

L'ICO evidenzia come il Regolamento generale sulla protezione dei dati ponga grande enfasi sulla documentazione che il titolare deve redigere e conservare per dimostrare la propria accountability.

La compliance agli step evidenziati dall'ICO, richiederà a enti e imprese di rivedere la governance, e il modo in cui gestiscono la protezione dei dati: qui mi pare opportuno richiamare, data la nostra scarsa familiarità con l'accountability, quanto detto dal Garante Europeo Giovanni Buttareli in una recente intervista: "Ai titolari del trattamento nel settore

pubblico e privato sarà richiesto non semplicemente di rispettare le norme, e quindi di fare una check-list degli adempimenti minimi, ma di tradurre in pratica questi princìpi con diversi "compiti a casa" in chiave di creatività e proattività. Dovranno dimostrare di aver distribuito responsabilità al proprio interno, di avere una risposta per i vari problemi, di aver valutato i rischi e le possibili conseguenze, e di quindi avere una strategia articolata e trasparente nei confronti dei soggetti cui si riferiscono le informazioni. Non sarà più una materia delegabile a un funzionario di turno, a un esperto di tecnologia o a un ufficio legale; sarà proprio l'approccio corporate che avrà importanza, anche perché si dovranno individuare anche linee di bilancio importanti." Anche l'ICO evidenzia "l'approccio corporate" suggerendo che uno degli aspetti che da ciò discendono potrebbe essere la revisione della contrattualistica e in generale degli accordi che regolano la condivisione o lo scambio di dati personali con altri soggetti (imprese, enti o professionisti).

L'ICO avverte anche che alcune norme potrebbero avere impatto diverso su diversi attori, ad esempio quelle sulla profilazione o sul trattamento dei dati dei minori, a seconda delle attività concretamente svolte. L'ICO dà quindi un ottimo suggerimento: mappare i trattamenti e le parti del Regolamento destinate ad avere maggiore impatto sul modello di business adottato e dare a questi aspetti un rilievo prioritario nella pianificazione dell'adeguamento.

Per provare a rispettare il pragmatismo dell'ICO ho usato nel prosieguo il termine "ente" nella sua accezione più ampia, in modo che potesse ricomprendere sia le persone giuridiche che gli organismi di diritto pubblico sia le associazioni che qualunque altra organizzazione impreditoriale, senza scendere in distinguo inutili ai fini che interessano.

1. Consapevolezza

Il primo passo da fare, secondo l'ICO è essere certi che i vertici e le persone chiave (di un ente pubblico o privato), e in generale chi ha potere decisionale, sappiano che la normativa sta cambiando e occorre virare verso il Regolamento generale sulla protezione dei dati.

Nelle strutture che, in Italia, abbiano provveduto alla nomina dei Responsabili (anche interni), la ricognizione delle figure decisionali e degli ambiti dei trattamenti sarà certamente più agevole.

È necessario, infatti, valutare l'impatto che il Regolamento potrebbe avere e identificare le aree che potrebbero dare maggiori problemi di compliance. L'analisi potrebbe partire dall'identificazione dei dei rischi, e chi ha già implementato procedure di mappatura parte avvantaggiato (chi non l'ha fatto può trovare utili suggerimenti qui).

Come già detto, soprattutto nelle realtà più grandi e complesse, l'adeguamento al Regolamento generale sulla protezione dei dati potrebbe comportare un certo sforzo: la prima parte del biennio di vacatio, pertanto, potrebbe essere dedicata proprio ad approfondire la conoscenza delle modifiche in arrivo; una lettura frettolosa dell'ultimo minuto potrebbe essere foriera di inciampi e intoppi, o di errori fatali.

Un aiuto in questa fase, in Italia, può giungere anche dall'organigramma privacy e dalle nomine a responsabile: per chi vi ha provveduto sarà facile comprendere chi prende le decisioni in ordine ai diversi trattamenti.

COSA FARE IN SINTESI

Accertarsi che le persone chiave delle struttura organizzativa del Titolare siano consapevoli dell'impatto che avrà il Regolamento, mappare le aree di rischio, individuare quelle che saranno maggiormente interessate dai cambiamenti e i ruoli decisionali; potrebbe essere necessario introdurre nuovi documenti (si pensi ad esempio al Registro dei trattamenti), interfacciarsi con nuove figure professionali (si pensi al Data Protection Officer), o intervenire sulla contrattualistica. Il primo passo è sapere cosa fare e chi dovrà farlo.

2. Dati trattati

L'ICO suggerisce di documentare quali dati si trattano, da dove si originano, e a chi vengono comunicati. La nostra normativa prevede già che il titolare tenga traccia di tali elementi e molte realtà continuano ad adottare documenti che "fotografano" i trattamenti anche dopo che è venuto meno l'obbligo di redigere o aggiornare il DPS (se lo avete archivio, potrebbe essere il momento di rispolverarlo: in questa fase propedeutica potrebbe tornare utile). L'ICO suggerisce

anche di pianificare procedure di verifica ("information audit") che coinvolgano l'intera struttura o solo per particolari aree.

Anche in questo caso, grazie alla severa scansione dei ruoli interni, per i titolari italiani di dimensioni contenute non dovrebbero esserci grosse difficoltà: le nomine a incaricato potranno essere utili nel ricostruire i trattamenti operati, le misure di sicurezza applicate, i flussi di dati.

Quindi, il primo step è individuare dati e informazioni, riconoscendo i dati personali: è dato personale secondo il Regolamento generale sulla protezione dei dati (art.4) "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Occorre fare attenzione perché la definizione non ricalca esattamente la precedente, è più ampia di quella della Direttiva. Il nostro legislatore, tuttavia aveva utilizzato un'espressione ben più generale e astratta del legislatore europeo. Anche questa volta, molti dei dati che in UE potevano destare dubbi applicativi, in Italia erano già stati considerati nel novero dei dati personali.

Occorrerà anche fare attenzione alla tipologia di dati trattati: il Regolamento definisce, sempre all'articolo 4 «dati genetici»,«dati biometrici», «dati relativi alla salute», mentre all'articolo 9 disciplina e definisce quelli a noi noti come "dati sensibili", ossia "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" che, sottoposti alla medesima disciplina prevista per i dati genetici, e i dati biometrici intesi a identificare in modo univoco una persona fisica, vengono (tutti) rubricati come "Trattamento di categorie particolari di dati personali" (si tratta quindi di un aggiornamento dell'articolo 8 della Direttiva 95/46/CE)

Una volta focalizzati i dati personali, occorre verificarne l'origine e seguirne i flussi. Il Regolamento aggiorna i diritti, parametrandoli al mondo interconnesso, enfatizzando gli obblighi documentali in ottica di accountability, in modo che il Titolare possa dimostrare la propria aderenza ai principi fondamentali del Regolamento. In particolare occorre porre l'attenzione sui flussi di dati e la loro condivisione (che si ha quando una organizzazione condivide i dati personali con altri). Il Regolamento, secondo l'ICO, impone di far comprendere la natura della condivisione, ad esempio documentando quali dati sono condivisi e quali misure organizzative vengono prese rispetto a questi dati. L'ICO porta un esempio che può essere efficace: se si hanno dati inesatti (o non aggiornati) e vengono condivisi con un altro organismo, bisognerà avvertire quest'ultimo delle carenze riscontrate in modo che possa aggiornarli. Tuttavia è impossibile fare una cosa del genere se non sappiamo che dati abbiamo, di che tipo, da dove arrivano, a chi li comunichiamo. E sarà bene tenere una traccia documentale di queste informazioni che abbiamo raccolto sui nostri trattamenti. Fare tutte queste cose, infatti, può aiutarci a soddisfare il principio di responsabilizzazione (accountability), che richiede ai Titolari di essere in grado di dimostrare di aver ottemperato ai principi che presiedono alla protezione dei dati (art. 5 del Regolamento generale sulla protezione dei dati), ad esempio adottando linee di condotta e procedure efficaci.

COSA FARE IN SINTESI

Documentare i dati personali trattati, da dove arrivano e con chi vengono condivisi.

Organizzare procedure di verifica, se necessarie.

3. Informative

Occorre rivedere le informazione rese agli interessati in modo da poterne pianificare l'aggiornamento o l'integrazione in tempo per il momento in cui il Regolamento generale sulla protezione dei dati sarà applicabile. L'obbligo di rendere l'informativa sussiste già oggi, e in Italia taluni elementi sono stati integrati anche da provvedimenti generali del Garante, quindi siamo abituati a rendere informative molto esaustive, ma il Regolamento aggiunge nuovi elementi a quelli già previsti dalla Direttiva (sulla quale si fondava l'articolo 13 del nostro Codice della

Privacy). Ad esempio, si dovrà spiegare all'interessato la base giuridica del trattamento (cfr successivo punto 6) o lo si dovrà informare dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, dovranno essere fornite informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze di tale trattamento previste per l'interessato (sebbene da noi l'informativa per la profilazione fosse già dovuta, si noterà che non è identica) o, ancora, si dovrà informare l'interessato circa la durata della conservazione dei suoi dati. Se l'interessato ritiene che ci siano delle irregolarità nel modo in cui il titolare gestisce i suoi dati ha diritto di adire l'Autorità: occorrerà informare l'interessato circa il suo diritto di proporre reclamo a un'Autorità di controllo; quindi dire all'interessato anche dove si trova e qual è l'Autorità alla quale si può rivolgere.

Le informazioni dovranno essere date in maniera semplice: occorrerà eliminare dalle informative gli inutili bizantinismi, preferendo forme schematiche di immediata comprensione. Il nostro Garante aveva già incoraggiato l'adozione d informative semplici e facilmente intellegibili, anche se non sempre è stato ascoltato.

Attenzione: controllare l'origine dei dati è molto importante: quando, infatti, i dati non sono raccolti presso l'interessato occorre fornire informazioni specifiche, che non coincidono perfettamente con quelle da fornire nel caso in cui, invece, i dati siano stati raccolti direttamente presso l'interessato.

COSA FARE IN SINTESI

Rivedere le informative e pianificare le modifiche necessarie prima della completa applicazione del Regolamento.

4. Diritti dell'interessato

Occorrerà che titolari e responsabili controllino le loro procedure in modo da poter garantire l'effettività dei diritti dell'interessato, incluso il diritto alla cancellazione dei dati e la possibilità di fornire i dati all'interessato a sua richiesta, in formato elettronico, di uso comune.

I principali diritti di cui gode l'interessato sotto il Regolamento generale sulla protezione dei dati sono:

1. diritto di accesso;
2. diritto alla correzione dei dati inesatti o non aggiornati;
3. diritto alla cancellazione delle informazioni;
4. diritto di sottrarsi al marketing diretto;
5. diritto di sottrarsi a decisioni automatizzate e profilazione.
6. diritto alla portabilità dei dati.

Buona parte dei diritti di cui gli interessati godranno durante la vigenza del Regolamento generale sulla protezione dei dati saranno gli stessi di cui godevano già con la Direttiva 95/46/CE, ma ci sarà un aumento delle garanzie. Per chi già oggi ha implementato sistemi efficaci per assicurare il soddisfacimento dei diritti degli interessanti, il passaggio dovrebbe essere più facile.

Per l'ICO è il momento di controllare le procedure, per migliorarle; è il momento di controllare come l'ente si pone di fronte all'esercizio dei diritti da parte dell'interessato: ad esempio, che succede in caso di richieste di cancellazione da parte dell'interessato? I sistemi in uso aiutano a reperire e cancellare i dati? Chi è che prende le decisioni in ordine alla cancellazione? Il diritto alla cancellazione, infatti è stato rivitalizzato dall'introduzione del "diritto all'oblio", riconosciuto all'interessato dall'articolo 17 del Regolamento, che deve essere soddisfatto tempestivamente o come dice il Regolamento "senza ingiustificato ritardo".

Il diritto alla portabilità dei dati è nuovo: in determinate circostanze si dovrà far fronte alla richiesta di portabilità avanzata dall'interessato. Nei casi in cui si debbano fornire i dati personali all'interessato occorrerà farlo in formato elettronico di uso comune. Molte imprese già hanno adottato forme di portabilità (si pensi ai contratti cloud) ma se questi vengono forniti in cartaceo o in formati elettronici non di uso comune l'ICO suggerisce di rivedere le procedure ed effettuare i necessari cambiamenti.

COSA FARE IN SINTESI

Controllare le proprie procedure in modo da assicurarsi che coprano tutti i diritti degli interessati, compresa la cancellazione e la possibilità di fornire i dati in un formato elettronico di uso comune.

5. Istanze di accesso da parte dell'interessato

I titolari dovranno controllare il modo in cui fronteggiano e riscontrano le istanze di accesso, in considerazione dei nuovi termini accodati dal Regolamento generale sulla protezione dei dati e delle informazioni aggiuntive rispetto al passato che occorrerà fornire.

Il Regolamento, infatti, introduce alcune modifiche in quest'ambito, ma nella maggior parte dei casi i titolari non dovrebbero avere necessità di cambiare il proprio approccio, dato che il Regolamento estende il termine quindicinale previsto dal nostro Codice della Privacy, raddoppiandolo. Il termine per riscontrare le richieste viene portato a un mese, come regola generale. Vi sono dei casi nei quali il titolare potrebbe non dar seguito alle richieste dell'interessato: ad esempio, quando esse siano manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo. Tuttavia incombe sul titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Tradotto in termini pratici dall'ICO, significa che se il titolare vuole opporre il rifiuto alle istanze dell'interessato dovrà adottare policy e procedure che gli consentano di dimostrare con trasparenza i parametri su cui poggia il suo rifiuto.

Il titolare dovrà anche riscontrare le istanze fornendo molteplici informazioni, come, ad esempio, in ordine al periodo di conservazione e al diritto alla correzione dei dati inesatti. Fronteggiare un ampio numero di istanze, considerata anche la mole di informazioni da fornire, potrebbe causare problemi organizzativi: in questi casi, suggerisce l'ICO, potrebbe essere il caso di valutare l'opportunità di sviluppare sistemi che consentano agli interessati di accedere facilmente online alle informazioni che li riguardano, anche al costo di sobbarcarsi spese ingenti per introdurre simili possibilità. Gli enti dovrebbero fare un'attenta analisi di costi e benefici sul lungo termine.

COSA FARE IN SINTESI

Aggiornare le proprie procedure in modo da poter riscontrare le istanze nei tempi previsti, valutare le ipotesi e adottare policy e procedure che consentano di giustificare il diniego.

6. Base giuridica del trattamento

I titolari dovranno esaminare i vari tipi di trattamento che operano, individuarne la base giuridica e documentarla.

Con il Regolamento, alcuni diritti degli interessati sono stati modificati in ragione della base giuridica del trattamento: ad esempio, è stato rafforzato il diritto alla cancellazione dei dati per i trattamenti la cui base giuridica è rappresentata dal consenso.

Attenzione: il consenso, per il Regolamento, non può costituire la base giuridica del trattamento qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente. È necessario, in questi casi, individuare una diversa base giuridica per proseguire i trattamenti.

Non solo: la base giuridica è tra gli elementi essenziali dell'informativa e deve essere evidenziata in riscontro a un'istanza di accesso. Le basi giuridiche dei trattamenti sono grosso modo le stesse della precedente direttiva e un esame attento dei trattamenti dovrebbe consentirne facilmente l'individuazione. La loro documentazione, invece, è necessitata dall'esigenza di fronteggiare gli obblighi che discendono dall'accountability.

Tra le basi giuridiche del trattamento si annovera anche il legittimo interesse: in particolare il legittimo interesse del titolare può costituire le base giuridica del trattamento a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (in particolare se l'interessato è un minore), tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbe sussistere tale legittimo interesse quando esista una relazione pertinente e appropriata tra l'interessato e il

titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali.

Occorrerà valutare molto attentamente tale presupposto, perché, a differenza di altri paesi non siamo abituati a una valutazione autonoma. Il bilanciamento degli interessi, nel nostro ordinamento era demandato all'Autorità Garante, pertanto per noi si tratta, in certa misura, di una novità.

COSA FARE IN SINTESI

Fare una ricognizione dei diversi trattamenti, individuandone la base giuridica per poterla comunicare (quando richiesto dalla normativa) e documentare.

7. Consenso

Questa è probabilmente l'area dove i titolari italiani sono maggiormente avvantaggiati, in quanto da sempre sottoposti a regole stringenti: il nostro Codice della Privacy ammette solo il consenso esplicito, e specifico per ogni finalità.

Ma di certo non può far male ricontrollare come i consensi vengono chiesti, ottenuti e registrati.

Il Regolamento generale per la protezione dei dati fa riferimento sia al "consenso" che al "consenso esplicito". Il consenso esplicito costituisce la base giuridica del trattamento di alcune tipologie di dati, come i dati afferenti alla salute, o nei processi decisionali automatizzati. In italia, per i dati "sensibili" (cfr. sopra n. 2) era necessario raccogliere il consenso scritto. La differenza nella acquisizione delle due tipologie di consenso posta dal Regolamento non è chiarissima, e

occorrerà attendere per valutare come vada implementata; sicuramente è richiesto uno standard elevato, dato che entrambi consistono in una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato.

Il consenso che non è definito "esplicito" deve infatti comunque rappresentare una manifestazione di assenso al trattamento da parte dell'interessato mediante dichiarazione o azione positiva inequivocabile e non può essere desunto dal silenzio, da form preflaggati o dalla mera inattività.

Se un trattamento è basato sul consenso (inequivocabile o esplicito), dovrà comunque rispondere a tutti questi requisiti. È importante ricordare che i diritti dell'interessato, per i trattamenti fondati sul consenso, sono particolarmente acuti e occorre che l'ente sia in grado di garantirne il soddisfacimento.

Il Regolamento chiarisce che i titolari devono essere in grado di dimostrare (e anche provare) la prestazione del consenso: sarà bene verificare il modo con cui i consensi vengono acquisiti e registrati, così da predisporre un efficace iter di controllo.

COSA FARE IN SINTESI

Rivedere in quali casi e con quali modalità vengono richiesti, ottenuti e registrati i consensi, in modo da valutare se sia necessario operare modifiche.

Valutare il valore probatorio della registrazione dei consensi in caso di controversie.

8. Minori

Cambiano le regole sul consenso dei minori, sarà bene, pertanto, cominciare a pensare a come realizzare sistemi di verifica dell'identità degli utenti, e a come garantirsi il consenso dei genitori o di chi ne fa le veci, per poter procedere ai trattamenti.

Il Regolamento generale sulla protezione dei dati appronta per la prima volta un regime di tutela speciale per i dati personali dei minori, in particolare per quanto riguarda il loro utilizzo a fini di marketing o di profilazione e la loro raccolta all'atto dell'utilizzo di servizi forniti direttamente a un minore, ad esempio servizi di social network.

Pertanto se un ente tratta dati di minori, occorrerà che presti attenzione al limite di età fissato per una valida prestazione del consenso, dotandosi di mezzi che permettano, ove necessario, di acquisire il consenso dei genitori (o di chi ne fa le veci), in modo da potere trattare i dati del minore nel rispetto della normativa. È importante evidenziare che il rapporto tra rischi e dati richiesti o procedure di verifica dell'identità deve essere rispettoso del principio di proporzionalità, da valutare anche in relazione alle circostanze o alla particolare area di trattamento.

Il Regolamento generale sulla protezione dei dati prevede un range entro il quale gli Stati membri potranno determinare l'età al raggiungimento della quale si potrà prestare validamente il consenso: esso é compreso tra i 13 e i 16 anni. Ogni Stato potrà determinare il proprio limite con legge nazionale, questo aspetto non è stato del tutto uniformato, pertanto, si dovrà prestare attenzione alle diverse normative.

L'ICO aggiunge un'ulteriore annotazione: il consenso deve essere sempre verificabile; per ottenere il consenso informato valido, occorre che l'informativa sia comprensibile per il minore, cioè sia scritta con un linguaggio che il minore possa capire.

COSA FARE IN SINTESI

Occorre valutare la predisposizione di sistemi che consentano la verifica dell'identità dei minori e garantiscano l'acquisizione del consenso da parte del "titolare della responsabilità genitoriale".

Valutare la possibilità di integrazione con il Regolamento eIDAS

9. Data breaches

Tutti dovrebbero assicurarsi di porre in essere procedure che consentano di individuare, riportare e investigare le violazioni di dati personali.

In Italia, in alcuni casi è già previsto che particolari categorie di titolari comunichino al Garante le violazioni subite. Tuttavia gli obblighi di comunicazione di violazioni all'Autorità, imposti dal Regolamento, si estendono a tutti i titolari, seppure al ricorrere di determinate condizioni, e ciò rappresenta a una novità assoluta per la stragrande maggioranza di essi. Occorrerà assicurarsi di avere adottato procedure idonee a scoprire eventuali violazioni, generare adeguata reportistica, e indagarne le cause e gli effetti. Ciò può importare una ricognizione dei dati coinvolti nei trattamenti operati, evidenziando quelli non sottoposti all'obbligo di comunicazione di data breach. Inoltre, quando la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve comunicare la violazione all'interessato senza ingiustificato ritardo. Ciò accade ad esempio quando la perdita di dati possa esporre gli interessati a perdite finanziarie. Queste comunicazioni vanno effettuate in breve tempo, e possono essere concomitanti e coinvolgere anche un importante numero di interessati: sarà opportuno predisporre idonee procedure e modulistica e aggiornare i dati degli interessati ai quali eventuali violazioni andrebbero comunicate. Non solo: le comunicazioni agli interessati non possono ricalcare quelle effettuate all'Autorità di controllo, ma dovranno essere epurate di tecnicismi e legalese, dato che il Regolamento stesso prevede che le comunicazioni agli interessati debbano adottare un linguaggio semplice e a loro immediatamente comprensibile. Le realtà più grandi dovrebbero implementare queste procedure sia a livello centrale che periferico, in modo da garantirne la tempestività.

Non solo: il titolare del trattamento deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i rimedi adottati. Tale documentazione consentirà all'autorità di controllo di verificare il rispetto delle prescrizioni normative.

È importante che soprattutto i comparti IT siano posti in condizione di operare rapidamente in caso di violazioni, in modo da prendere le precauzioni necessarie e consentire di assolvere agli obblighi di comunicazione connessi nel rispetto dei termini assegnati dal legislatore.

La violazione delle norme sulla comunicazione di data breach espone il titolare e il responsabile a sanzioni autonome che si affiancano a quelle eventualmente comminabili per la violazione di dati stessa.

COSA FARE IN SINTESI

Occorre accertarsi di avere procedure efficaci che consentano di individuare, documentare investigare e (se necessario) comunicare, come per legge, le violazioni di dati personali.

10. Protezione dei dati sin dalla progettazione e valutazione d'impatto sulla protezione dei dati

Qui l'ICO invita a familiarizzare con la guida che egli stesso ha predisposto tempo fa per le "Privacy Impact Assessments" (PIAs) allo scopo di implementarle ciascuno nella propria realtà.

La guida ha il pregio di far comprendere, anche a noi italiani, come la Valutazione di impatto sulla protezione dei dati possa collegarsi ad altre procedure organizzative quali la gestione dei rischi o il project management. Il punto di partenza é una valutazione delle situazioni per le quali si renderebbe necessario condurre una DPIA (valutazione di impatto sulla protezione dei dati). Chi la farà? Chi altri dovrebbe parteciparvi? Il processo dovrebbe svolgersi a livello centrale o a livello locale?

Molto interessante è la prospettiva dell'ICO, per il quale é sempre stata una buona pratica adottare un approccio orientato alla privacy by design nel cui ambito condurre la valutazione di impatto privacy (PIA).

La collocazione della PIA nell'ambito della Privacy by design aiuta certamente a sfuggire da assiomi astratti, o burocratizzazione degli adempimenti, in favore di una applicazione concreta di immediata percezione.

Prediligere la privacy by design e la minimizzazione dei dati non é una novità assoluta: il Regolamento generale sulla protezione dei dati ha esplicitato requisiti che erano insiti nei principi generali che presiedevano già alla protezione dei dati. La differenza tra PIA e DPIA sarebbe più che altro terminologica.

L'ICO sottolinea come non è sempre necessario condurre una PIA: la valutazione di impatto privacy é richiesta in situazioni che presentano rischi elevati, ad esempio quando si sviluppa una nuova tecnologia o quando operazioni di profilazione possano incidere significativamente sugli interessati. Saranno le Autorità nazionali, anche in coordinamento tra loro, a definire le tipologie di trattamenti da sottoporre o sottrarre alla valutazione di impatto sulla protezione dei dati.

Se la PIA indica trattamenti ad alto rischio, si dovrà consultare l'Autorità competente, in modo che possa emettere un parere indicando se il trattamento sia conforme al Regolamento.

COSA FARE IN SINTESI

Bisognerebbe prendere confidenza con le valutazioni di impatto sulla protezione dei dati come prima cosa, in modo da comprendere come e quando implementarle. In assenza di fonti nazionali specifiche sarà utile allo scopo consultare sia il sito dell'ICO, sia il parere reso dal WP ex art 29 n. 04/2013 concernente il modello di valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti, nonché la sua implementazione; leggere il parere del Garante europeo; monitorare il WP29, tenendo conto che nell'Agenda del 2016 del Gruppo di Lavoro ex art 29 è prevista l'elaborazione di linee guida per la DPIA.

11. Data Protection Officer

In determinate circostanze sarà necessario designare il DPO o responsabile della protezione dei dati. In tali casi occorrerà rendere questo ruolo compatibile con il proprio assetto organizzativo.

Potrà essere utile per farsi una prima idea l'apposita scheda predisposta dal Garante Privacy.

Il Regolamento prevede che alcuni enti debbano designare un DPO, ad esempio le autorità pubbliche o coloro le cui le attività principali consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; la cosa importante è che o qualcuno all'interno dell'organizzazione o un consulente esterno si assuma le necessarie responsabilità in ordine alla conformità dei trattamenti e abbia il patrimonio di conoscenze, il sostegno e l'autorità per poterlo fare in maniera efficace.

Occorre tener presente, inoltre, che le indicazioni fornite da un responsabile della protezione dei dati servono a orientare titolari e responsabili sulle misure da prendere in ordine all'esistenza e alla valutazione dei rischi connessi al trattamento nonché sull'individuazione di prassi volte ad attenuarli, e servono, al pari d certificazioni e codici di condotta, a dimostrare la conformità dei trattamenti da parte del titolare del trattamento o dal responsabile del trattamento (mitigandone le responsabilità).

E' importante garantire al DPO di poter adempiere ai propri compiti e funzioni in maniera indipendente, sia che egli sia un soggetto esterno, sia che egli sia un dipendente del titolare o del responsabile. In ogni caso, potrebbero essere necessari interventi sui ruoli , sulle gerarchie e sulla governance aziendale, dato che da un lato, il DPO deve godere di indipendenza, dall'altro deve potersi interfacciare con i ruoli chiave in tema di protezione dei dati personali, anche di vertice. In altre parole il DPO deve essere messo in condizione di dialogare con chi siede ai posti di comando e prende le decisioni, in modo da poter spiegare i rischi connessi ai trattamenti e suggerire le misure da prendere. Egli deve poter esercitare la propria influenza su policy e procedure, in modo da garantire una conformità effettiva ai requisiti imposti dal Regolamento.

La cosa migliore da fare al momento, comunque, é comprendere se si rientri nel novero dei soggetti obbligati a dotarsi di un DPO, e, nel caso, valutare se il proprio approccio, anche strutturale, alla protezione dei dati soddisfa i requisiti richiesti dal Regolamento generale sulla protezione dei dati, in attesa che il Gruppo di Lavoro ex art. 29 fornisca indicazioni più precise.

COSA FARE IN SINTESI

Valutare se si rientra nei casi previsti dalla normativa per cui occorre designare un DPO al fine di dimostrare la conformità ai requisiti di sicurezza previsti dal Regolamento, e valutare come questo ruolo potrà collocarsi in rapporto alla propria struttura, considerando le necessarie modifiche anche in ordine alla governance.

12. Trattamenti transfrontalieri

Se si opera a livello internazionale occorre comprendere sotto quale Autorità nazionale si ricade.

Il Regolamento elabora in maniera piuttosto complessa il modo in cui una Autorità (quella nel cui territorio ricade lo stabilimento principale del Titolare) diviene "capofila", nel caso di controlli su trattamenti transfrontalieri, ad esempio quando operazioni di trattamento incidano su interessati di diversi Stati membri. L'Autorità capofila si individua sulla base dello stabilimento principale del titolare. Quello di "stabilimento principale" è un concetto nuovo, introdotto dal Regolamento; con la direttiva era sufficiente l'individuazione dello stabilimento ai soli fini dell'applicazione delle diverse normative nazionali.

Lo stabilimento principale di un titolare del trattamento è il luogo in cui ha sede la sua amministrazione centrale nell'Unione, a meno che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione, nel qual caso lo stabilimento principale è quello in cui vengono prese le decisioni. Nelle realtà più complesse non è sempre agevole individuare o stabilimento principale, dato che i diversi trattamenti possono essere effettuati e decisi in luoghi diversi: sarà utile, in questi

casi, mappare dove vengono prese le decisioni più importanti in ordine alla protezione dei dati, in modo da risalire all'Autorità capofila.

L'individuazione dello stabilimento principale, pertanto determina l'individuazione dell'Autoritá che sarà competente come capofila in caso di controlli e sanzioni.

COSA FARE IN SINTESI

Se si opera in più Stati e si hanno diversi stabilimenti occorre mappare i nodi decisionali per determinare sotto quale Autorità per la protezione dei dati si ricade.

13. Non dimentichiamo l'accountability

L'ICO suggerisce 12 step, ma io vorrei aggiungerne uno a corredo di quanto accennato in introduzione. Più volte, nel corso di questa breve analisi, si è fatto riferimento all'accoutability (o responsabilizzazione). L'ICO non le dedica uno step tutto suo, limitandosi a sottolinearne le interferenze con gli altri punti trattati, probabilmente perché è un istituto che ritiene già noto ai titolari di matrice anglosassone. Tuttavia essa rappresenta probabilmente la maggiore novità per noi italiani e, a mio avviso, la più importante. Non aggiungerò molto alla descrizione già fornita dal dottor Buttarelli, che mi pare molto efficace. Aggiungo soltanto che l'EDPS, ossia l'ufficio del Garante Europeo, che il dottor Buttarelli presiede, nel 2015 ha avviato un'importante iniziativa volta a sviluppare un modello che consentisse di garantire l'accountability nei trattamenti di dati personali. Il modello è stato applicato all'Autorità stessa, e ora viene diffuso, affinché possano prendervi spunto anche le altre istituzioni europee. Seppure sia pensato per un organismo pubblico di stampo europeo, può certamente essere di ispirazione anche ai titolari privati che operano nel nostro Paese.

COSA FARE IN SINTESI

Leggere il questionario allegato alla "Accountability initiative" del Garante Europeo, in modo da familiarizzare con il principio di responsabilizzazione e trarne spunto per la propria struttura.