CONFINDUSTRIA

Position Paper

GDPR: alcune considerazioni di Confindustria al Legislatore delegato

Febbraio 2018

Confindustria ritiene necessaria l'attuazione della delega (art. 13 della legge n. 163/2017) per l'adeguamento della normativa nazionale alle disposizioni del nuovo Regolamento europeo sulla protezione dei dati personali (n. 679/2016, di seguito: "GDPR" o "Regolamento").

Infatti, al fine di assicurare la certezza del quadro giuridico di riferimento e agevolare gli operatori italiani nell'implementazione delle nuove norme, risulta fondamentale riordinare la disciplina interna in tema di privacy e allinearla alle previsioni del Regolamento.

Quanto ai **tempi dell'attività di riordino normativo**, si ribadisce l'esigenza, più volte rappresentata al Governo, di accelerare l'adozione dei decreti delegati. Come noto, la delega scadrà il 21 maggio 2018, in concomitanza con l'entrata in operatività del GDPR (25 maggio 2018), pertanto, l'auspicio delle imprese è di avere a disposizione un tempo adeguato per ottemperare alle previsioni del Legislatore nazionale.

Quanto al **metodo**, è innanzitutto necessario che l'attività di adeguamento nazionale sia condotta in coordinamento con gli altri Stati membri dell'UE, al fine di preservare l'armonizzazione delle norme in tema di privacy che lo stesso GDPR mira a realizzare. Infatti, un potenziale *gold plating* in ambito privacy potrebbe compromettere la libera circolazione dei dati e ostacolare il funzionamento del mercato interno, nonché disincentivare gli investimenti nel nostro Paese. Pertanto, è importante limitare l'intervento nazionale ai profili strettamente necessari, evitando di introdurre a carico delle imprese italiane oneri e adempimenti non indispensabili ai fini della protezione dei dati personali.

In secondo luogo, Confindustria rinnova al Legislatore delegato l'invito - che lo stesso Regolamento porge alle Istituzioni europee e nazionali coinvolte nella sua implementazione - di *considerare le esigenze specifiche delle micro, piccole e medie imprese* nell'applicazione delle nuove regole (Considerando 13 del GDPR).

Come noto, il GDPR introduce il principio della responsabilizzazione, cd. *accoutability,* che trasforma la *compliance* privacy da adempimento normativo a sistema di gestione: le imprese sono chiamate a valutare, adeguare e dimostrare la conformità dei trattamenti che realizzano al Regolamento, nonché a mutare il proprio approccio alla protezione dei dati personali. L'attuazione di tale nuovo approccio richiede un significativo sforzo culturale e operativo, al quale non tutti gli operatori sono in grado di provvedere, soprattutto in termini economici. Pertanto, è fondamentale alleggerire il più possibile il peso degli oneri di adeguamento sulle imprese e individuare soluzioni "sostenibili" da parte degli operatori più piccoli.

Quanto al **merito dell'attività di riordino normativo**, di seguito alcune considerazioni sull'implementazione dei principi e dei criteri cui il Legislatore delegato dovrà attenersi nell'attuazione della delega.

In primo luogo, il Legislatore delegato dovrebbe abrogare espressamente le disposizioni del D.Lgs n. 196/2003 (di seguito: "Codice privacy") superate dal Regolamento (l'art. 94 del GDPR abroga espressamente la Direttiva 95/46/CE) e confermare quelle compatibili con il nuovo regime.

Con riferimento a queste ultime, Confindustria ritiene che siano in linea con lo spirito del GDPR e che, pertanto, possano essere mantenute in vigore:

- l'ipotesi di esonero dal consenso relativa al trattamento dei dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque (art. 24, co. 1, lett. *c)* del Codice privacy);
- l'ipotesi di esonero dal consenso relativa al trattamento dei dati relativi allo svolgimento di un'attività economica (art. 24, co. 1, lett. *d)* del Codice privacy), idonea a legittimare l'utilizzo delle informazioni relative all'attività commerciale, imprenditoriale o professionale di un soggetto, compresi i profili organizzativi, amministrativi, produttivi, patrimoniali e finanziari di un'impresa (es. identità degli azionisti e numero di azioni di cui sono titolari). Inoltre, tale ipotesi di esonero assume rilevanza ai fini dei trattamenti in ambito B2B, aventi ad oggetto i dati degli imprenditori individuali;
- l'ipotesi di esonero dal consenso relativa al trattamento di dati comuni effettuato da associazioni, enti od organismi senza scopo di lucro in riferimento agli aderenti e ai soggetti che hanno con essi contatti regolari (art. 24, co. 1, lett. *h)* del Codice privacy), che lo stesso GDPR ha previsto solo con riferimento al trattamento di categorie particolari di dati (art. 9, par. 2, lett. *d)* del GDPR);
- l'ipotesi di esonero dal consenso relativa alla comunicazione dei dati infragruppo per finalità amministrativo-contabili, da intendersi peraltro come espressione - riconosciuta in via legislativa - del perseguimento di un legittimo interesse del titolare. (art. 24, co. 1, lett. *i-ter)* del Codice privacy);
- la disciplina per il trattamento dei dati personali – comuni e particolari – contenuti nei CV spontaneamente inviati (artt. 13, co. 5-bis, 24, co. 1, lett. *i-bis)*, art. 26, co. 3, lett. *b-bis)* del Codice privacy);
- l'abilitazione *ex lege* al trattamento dei dati "giudiziari" effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata (art. 21, co. 1-*bis* e 27, co. 1 del Codice privacy). Tale previsione assume notevole rilevanza per l'implementazione del Protocollo di legalità che Confindustria ha stipulato con il Ministero dell'Interno al fine di rafforzare la collaborazione tra imprese e istituzioni nella prevenzione e il contrasto delle infiltrazioni della criminalità organizzata nell'economia.

In secondo luogo, il Legislatore delegato dovrebbe <u>valutare con attenzione se e come disciplinare gli ambiti sui quali Regolamento consente l'intervento degli Stati membri</u>.

Tra gli ambiti di maggior interesse per le imprese, si segnalano:

- i trattamenti dei dati nell'ambito del rapporto di lavoro (art. 88 del GDPR). Si tratta di una categoria di trattamenti di forte impatto per le imprese, rispetto ai quali sussiste una forte esigenza di semplificazione nella gestione degli adempimenti e di bilanciamento della tutela dei dati personali dei lavoratori con le analoghe garanzie già assicurate dalla disciplina lavoristica (es. artt. 4 e 8 dello Statuto dei lavoratori). Inoltre, con riferimento ai trattamenti connessi alla gestione del rapporto di lavoro, assume notevole rilevanza il concetto del *"perseguimento del legittimo interesse del titolare"* che, in linea con le indicazioni fornite dal WP29 (Parere n. 2/2017), costituisce una delle principali condizioni di liceità del trattamento. Come noto, il concetto di legittimo interesse nel nostro ordinamento non rappresenta una novità assoluta: il Codice privacy assegna al Garante privacy il potere di individuare il legittimo interesse del titolare a un certo trattamento, che può essere eseguito

senza acquisire il consenso degli interessati; la recente Legge di Bilancio 2018, poi, ha rafforzato i compiti dell'Autorità, prevedendo l'adozione di Linee guida sui trattamenti finalizzati al perseguimento di un interesse legittimo del titolare e realizzati con strumenti tecnologici e lo svolgimento di un controllo preliminare sugli stessi. Sul punto, si evidenzia come la previsione di un controllo *ex ante* dell'Autorità sullo svolgimento di un trattamento dei dati personali non appaia in linea con lo spirito del GDPR che, come anticipato, introduce l'*accountability* ed elimina ogni adempimento abilitativo preliminare (es. autorizzazione, notificazione, verifica preliminare) nei confronti del Garante privacy. Più coerente con il principio di responsabilizzazione, invece, risulta la previsione di Linee guida che, peraltro, risponde alla richiesta delle imprese di indicazioni e indirizzi sui trattamenti finalizzati al perseguimento di un legittimo interesse. Pertanto, l'invito che Confindustria rivolge al Legislatore delegato è di correggere la criticità introdotta dalla Legge di Bilancio 2018 in tema di trattamenti finalizzati al perseguimento di un legittimo interesse del titolare, eliminando il controllo preventivo del Garante privacy e confermando l'adozione di indicazioni e indirizzi da parte dell'Autorità;

- i trattamenti dei dati relativi alla salute, dei dati biometrici e dei dati genetici, per i quali gli Stati membri possono mantenere o introdurre condizioni o limitazioni (art. 9, par. 4 del GDPR). Si tratta di trattamenti a vario titolo connessi alla gestione del rapporto di lavoro e rispetto ai quali si ribadisce l'esigenza di semplificazione. Pertanto, al fine di alleggerire gli adempimenti privacy in ambito lavoristico, si invita il Legislatore delegato a non mantenere (es. consenso scritto e preventiva autorizzazione del Garante privacy per il trattamento dei dati relativi alla salute), estendere o introdurre ulteriori condizioni al trattamento dati relativi alla salute, dei dati biometrici e dei dati genetici, lasciando invariato il livello di tutela assicurato dal GDPR a questi trattamenti;
- i trattamenti dei dati "giudiziari" (art. 10 del GDPR), che rilevano sia ai fini dell'attuazione del citato Protocollo di legalità stipulato da Confindustria e il Ministero dell'Interno, che ai fini dell'implementazione di procedure di legalità interne all'impresa.

Un ulteriore aspetto da considerare nell'attività di adeguamento normativo è il ricorso ai provvedimenti del Garante privacy.

Il Regolamento prevede, fino alla loro modifica, sostituzione o abrogazione, il mantenimento delle autorizzazioni adottate dalle varie Autorità di controllo in virtù della Direttiva 95/46/CE (Considerando n. 171 del GDPR). Tuttavia, una simile reviviscenza non è prevista per i provvedimenti - generali, ma anche specifici - con i quali le Autorità di controllo nazionali hanno negli anni fornito prescrizioni e indicazioni in merito a particolari trattamenti e che costituiscono, in ogni caso, un punto di riferimento certo per le imprese titolari del trattamento. . Si pensi, ad esempio, a: Provvedimento 1 marzo 2007, recante le Linee Guida per l'utilizzo della posta elettronica e internet; Provvedimento 27 novembre 2008, in materia di amministratore di sistema; Provvedimento 8 aprile 2010, in materia di trattamento di dati personali effettuato tramite sistemi di videosorveglianza; Provvedimento 4 ottobre 2011 sui sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro; Provvedimento 4 aprile 2013 in materia di *data breach*; Provvedimento 12 novembre 2014 in tema di biometria.

È, in ogni caso, importante avviare, sia con riferimento alle autorizzazioni generali, che ai provvedimenti del Garante privacy, un'attività di ricognizione e adeguamento al Regolamento, soprattutto rispetto agli adempimenti che il GDPR ha soppresso (es. notificazione, istanza di verifica preliminare), al fine di chiarire i presidi cui fare riferimento e confermare le soluzioni compatibili e consolidate.

Sempre con riferimento al ricorso alla sede amministrativa, si potrebbe demandare al Garante privacy l'individuazione di alcune semplificazioni per le micro, piccole e medie imprese, al fine di minimizzare l'impatto economico delle nuove norme. In particolare, in linea con il citato Considerando 13 del GDPR e i precedenti orientamenti dell'Autorità (es. Provvedimento 19 giugno 2008, 27 novembre 2008), si potrebbe demandare alla stessa la previsione di misure di semplificazione per l'adempimento dell'obbligo di informativa, lo svolgimento di attività di *marketing* diretto, l'istruzione del personale preposto al trattamento, nonché l'indicazione di misure di sicurezza adeguate allo svolgimento di determinati trattamenti (es. in base agli strumenti utilizzati o in ragione dei rischi effettivi per i diritti degli interessati).

Infine, con riferimento alle previsioni in materia sanzionatoria:

- in ambito penale, si auspica un approccio di depenalizzazione, considerato che ad oggi i reati preposti alla tutela del dato personale (es. art. 167del Codice privacy) hanno un carattere di sussidiarietà *("salvo che il fatto non costituisca reato più grave")* e che nell'ordinamento già sussistono altre fattispecie di reato a tutela del bene giuridico riservatezza (es. art. 326 cp violazione del segreto di ufficio, art. 38 dello Statuto dei lavoratori in tema di diritto pensale del lavoro – norma peraltro richiamata dallo stesso Codice privacy);
- in ambito amministrativo, occorre assicurare un'effettiva equità nell'applicazione delle sanzioni, nonché un'efficiente gestione dei procedimenti davanti al Garante privacy.