CONFINDUSTRIA

Regolamento UE sulla protezione dei dati personali: i principali punti di attenzione per le imprese

Giugno 2017

Regolamento europeo sulla protezione dei dati personali: i principali punti di attenzione per le imprese

1. Adeguamento normativo al Regolamento n. 679/2016 (di seguito, anche "GDPR")

1.1 Livello normativo primario: si ritiene assolutamente necessaria l'adozione di un atto legislativo interno volto a riordinare la disciplina nazionale in tema di protezione dei dati personali, mediante l'abrogazione espressa delle 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), al fine di assicurare la certezza del quadro giuridico di riferimento.

Quanto ai punti che il GDPR rimette all'intervento – in alcuni casi obbligatorio e in altri facoltativo – degli Stati membri, appare fondamentale una riflessione preliminare in merito agli ambiti sui quali procedere. Al riguardo, si segnalano quelli prioritari per le imprese:

- i trattamenti dei dati relativi alla salute, dei dati biometrici e dei dati genetici *ex* art. 9, co. 4 del GDPR, per la loro attinenza alla gestione del rapporto di lavoro e, con particolare riferimento ai dati relativi alla salute, per il superamento del più restrittivo regime oggi previsto dal Codice privacy (consenso scritto e preventiva autorizzazione del Garante privacy);
- i trattamenti in esecuzione di un obbligo di legge *ex* art. 6, co. 2 del GDPR;
- i trattamenti dei dati dei dipendenti nell'ambito del rapporto di lavoro *ex* art. 88 del GDPR;
- i trattamenti dei dati "giudiziari" *ex* art. 10 del GDPR. Quest'ultimo profilo assume notevole rilevanza per: *i)* dare attuazione al Protocollo di legalità che Confindustria ha stipulato con il Ministero della Giustizia e per il quale è oggi prevista una disposizione *ad hoc* - art. 21, co. 1-*bis* del Codice privacy, richiamato anche dall'art. 27, che appunto autorizza *ex lege* questo trattamento; *ii)* implementare procedure di legalità interne all'impresa sulle quali l'Autorità ha in corso confronti specifici con alcune imprese associate.

In ogni caso, è 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, cui lo stesso GDPR punta.

1.2 Livello normativo secondario: 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.

Sia con riferimento alle autorizzazioni generali che ai provvedimenti del Garante privacy, si ritiene fondamentale avviare 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.

2. Implementazione del Regolamento n. 679/2016

2.1 Osservazioni di carattere generale

Confindustria ha molto apprezzato l'attività che il Garante privacy sta realizzando a livello nazionale ed europeo (es. il mantenimento terminologico delle nozioni di Titolare e Responsabile del trattamento nella traduzione italiana del Regolamento; la Guida all'applicazione del Regolamento UE 2016/679 in materia di protezione dei dati personali, pubblicata il 28 aprile 2017, di seguito: "Guida"). L'auspicio è che il coinvolgimento delle associazioni imprenditoriali diventi strutturale, affinché ci sia un confronto preliminare sulle indicazioni che l'Autorità intende fornire alle imprese titolari del trattamento.

Sempre su un piano generale, è necessario semplificare il più possibile l'implementazione del Regolamento, curando l'armonizzazione cui il GDPR mira e, al tempo stesso, bilanciando l'*accountability* con l'attenzione alle esigenze di proporzionalità delle imprese più piccole, in osservanza del Considerando n. 13 del GDPR. A tal fine, potrebbe avviarsi un confronto su:

- **codici di condotta**. In ambito privacy, si registra una positiva esperienza di questi strumenti, soprattutto per la loro portata settoriale e la relativa valenza quale fonte del diritto (una volta sottoscritti, vengono adottati con decreto del Ministro della Giustizia, pubblicati in GU e riportati in allegato al Codice privacy);

- **certificazione**. Si registra un ritardo in merito all'accreditamento degli organismi di certificazione, che il GDPR rimette alle Autorità di controllo e all'organismo nazionale di accreditamento designato in virtù del Regolamento n. 765/2008;

considerato *che l'adesione ai codici di condotta … o a un meccanismo di certificazione … può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento* (art. 24, co. 3 del GDPR). Tuttavia, il GDPR non attribuisce efficacia esimente all'adozione di tali meccanismi.

In quest'ottica, poi, sarebbe auspicabile un chiarimento dell'Autorità in merito all'esclusione dei dati delle imprese individuali dall'ambito di applicazione del Regolamento, in modo da allineare il regime privacy a quello previsto per le altre tipologie di imprese. Il rischio derivante dalla lettura combinata della definizione di interessato (persona fisica) e del Considerando n. 14 del GDPR (*Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto*) è di assoggettare i trattamenti connessi all'esercizio dell'attività di impresa a due diverse procedure a seconda della forma giuridica rivestita dal soggetto cui si riferiscono i dati. Peraltro, da un'indagine condotta qualche anno fa, è emerso che nel Regno Unito e in Spagna le Autorità di controllo hanno assunto un orientamento che equipara ai fini privacy i dati dell'imprenditore individuale a quelli di una persona giuridica, escludendoli dalla disciplina di riferimento.

2.2 Osservazioni di dettaglio

Filiera privacy: sono diverse le perplessità in merito alla figura del Responsabile del trattamento (*cd*. *processor*) e, in particolare, alla sua configurabilità – in (dis)continuità con quanto oggi previsto dal Codice privacy - come soggetto interno alla struttura del Titolare (tali perplessità nascono principalmente dall'obbligatorietà della nomina di tale figura e dalla previsione della responsabilità solidale con il Titolare del trattamento).

Il GDPR sembra delineare il Responsabile del trattamento come una figura esterna all'organizzazione del Titolare: il Responsabile, infatti, è il soggetto che tratta i dati per conto del Titolare ed è destinatario di specifici obblighi (es. tenuta del registro; nomina del DPO; nomina del rappresentante). Questa impostazione risulta coerente con l'orientamento del WP29 (*Opinion* n. 1/2010), che inquadra il *processor* all'esterno dell'organizzazione del *controller* (Titolare), richiamando al riguardo i concetti di esternalizzazione e delega.

Sarebbe molto importante, sul punto, un chiarimento dell'Autorità, visto che la Guida non affronta tale questione, ma si limita a chiarire solo la portata dei concetti di Titolare e di Incaricato/persona autorizzata. In particolare, qualora dovesse confermarsi il superamento di tale figura interna, sarebbero auspicabili suggerimenti da parte dell'Autorità in ordine all'organizzazione della filiera privacy in ambito aziendale. Infatti, ad oggi, le imprese registrano una esperienza positiva in ordine al responsabile interno, considerato una sorta di intermediario tra il Titolare (*management*) e gli Incaricati.

Sempre con riferimento alla filiera privacy, sarebbe auspicabile la predisposizione da parte dell'Autorità di tracce o clausole contrattuali per la nomina del Responsabile del trattamento (art. 28, co. del GDPR) e per l'incarico alle persone autorizzate, che ogni Titolare possa poi personalizzare ovvero adattare alle specificità della propria organizzazione.

DPO: le Linee Guida del WP29 sollevano diversi dubbi in merito a:

1. i soggetti che hanno l'obbligo di nominare il DPO. Considerato che, sul piano generale, il WP29 incoraggia la designazione del DPO anche nei casi in cui tale figura non sia obbligatoria e che, anche se volontaria, la nomina del DPO deve essere necessariamente assistita dalle prerogative e dalle garanzie previste dal GDPR (con conseguenti costi ed eventuali sanzioni), appare fondamentale chiarire quando la scelta di avvalersi del DPO sia una scelta di obbligo o di opportunità. In particolare, sul piano soggettivo, sarebbe auspicabile un chiarimento in ordine alle società *cd*. "partecipate" dalla PA e a quelle che erogano pubblici servizi, per le quali il WP29 ritiene verosimile la necessità di nominare il DPO, ma non fornisce indicazioni in merito alle circostanze (dimensionali ovvero funzionali) che possono giustificare una scelta in senso negativo. Parimenti, sul piano oggettivo, sarebbe auspicabile un chiarimento in merito al rapporto tra il concetto di monitoraggio regolare e sistematico - cui è legato l'obbligo di nominare il DPO e che il WP29 individua anche nelle *"attività di marketing basate sull'analisi dei dati raccolti"* - e lo svolgimento di attività di *marketing*, in modo da escludere dall'ambito obbligatorio la mera attività di *marketing* diretto effettuata sulla base dei dati raccolti;
2. i "fattori pertinenti" su cui fondare l'eventuale scelta di non ricorrere a tale figura (es. tipologia di attività connessa al trattamento dei dati personali; organizzazione interna idonea a presidiare i rischi cui la figura del DPO è preposta). Anche sul punto sarebbero auspicabili maggiori indicazioni da parte dell'Autorità, al fine di confortare la valutazione delle imprese in ordine alla loro esclusione dal novero dei soggetti tenuti alla nomina del DPO;

3. la posizione del DPO e la sua collocazione nell'organigramma aziendale, posta la necessità di assicurare indipendenza e assenza di conflitto di interessi. Al riguardo, sarebbero utili dei suggerimenti da parte dell'Autorità, che consentano di introdurre la figura del DPO all'interno dei contesti aziendali senza stravolgere gli assetti organizzativi.

Informativa: vi sono alcune difficoltà nell'impostare un'informativa che sia allo stesso tempo esaustiva (completa di tutti gli elementi indicati dal GDPR), concisa e intellegibile. Al di là delle modalità che maggiormente si adattano al mondo virtuale, dove è possibile procedere a un'informativa "stratificata", quelle che destano più preoccupazione sono le modalità tradizionali.

Un'ulteriore preoccupazione è legata alla tempistica del trattamento che, rispetto ad oggi, dovrà essere indicata nell'informativa (o almeno i criteri per individuarla). Al riguardo, sarebbe importante ricevere indicazioni da parte del Garante privacy, al fine di indirizzare le imprese nell'individuazione di tempi di conservazione dei dati personali commisurati alle finalità perseguite. A tale fine, andrebbe privilegiato un approccio di semplificazione, in modo da facilitare la gestione interna delle informazioni e l'implementazione di procedure di agevole definizione.

Consenso: le maggiori preoccupazioni riguardano la "sopravvivenza" dei consensi acquisiti ai sensi del Codice privacy e l'incidenza dei nuovi contenuti dell'informativa ai fini della configurabilità di un consenso "conforme". Sul punto la Guida del Garante privacy non assume una posizione chiara, pertanto, si auspica l'attuazione di un approccio sostanziale e non formale.

Legittimo interesse: il GDPR ha confermato il perseguimento di un interesse legittimo del Titolare (o di un terzo) tra le condizioni di liceità del trattamento in assenza del consenso: l'individuazione di tale interesse e il suo bilanciamento con i diritti e le libertà degli interessati vengono rimessi direttamente al Titolare (il Codice privacy affida queste operazioni al Garante privacy). È importante fornire indicazioni più specifiche in merito al concetto di legittimo interesse (l'*Opinion* n. 6/2014 del WP29 non è chiara e la stessa Guida del Garante privacy si limita a richiamare sul punto i provvedimenti su videosorveglianza e biometria), soprattutto rispetto ai casi indicati dal GDPR:

1. potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento (es. rapporto B2C, rapporto di lavoro);

2. può essere considerato legittimo interesse trattare dati personali per finalità di *marketing* diretto. Sul punto, sarebbero auspicabili indicazioni in ordine alle casistiche ricomprese (dando per acquisite, anche ai sensi della Direttiva 2002/58/CE e dell'art. 130 del Codice privacy, le ipotesi di *soft spam*) e alla possibilità di associare il perseguimento di tale legittimo interesse alla profilazione;
3. trasmissione di dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti.

In tale contesto, poi, va esaminata la possibilità di ricondurre nel concetto di legittimo interesse alcuni vigenti casi di esonero dal consenso non confermati dal GDPR come, ad esempio, il trattamento riguardante dati relativi allo svolgimento di attività economica *ex* art. 24, co. 1, lett. *d)* del Codice privacy o il trattamento dei dati contenuti nei CV spontaneamente inviati *ex* art. 24, co. 1, lett. *i-bis)* del Codice privacy.

Registro del trattamento: apprezzabili le indicazioni contenute nella Guida del Garante privacy e l'intenzione di mettere a disposizione un modello di registro. Tuttavia, permane la necessità di chiarire maggiormente l'esonero per le imprese con meno di 250 dipendenti, visto che la formulazione del GDPR è ambigua. Sul punto, sarebbe opportuno precisare che l'esonero riguarda le imprese con meno di 250 dipendenti che trattano come unici dati "sensibili" e "giudiziari" quelli connessi alla gestione del rapporto di lavoro (infatti un'impresa anche con un solo dipendente tratta dati sensibili in maniera non occasionale, poiché tali dati sono connessi alla gestione del rapporto di lavoro).

Misure di sicurezza: anche sotto questo profilo, è forte la richiesta delle imprese in merito a indicazioni da parte dell'Autorità. Pertanto, si accoglie con favore l'intenzione di definire linee guida e buone prassi, partendo però da quanto già previsto – e implementato dalle imprese – dal Disciplinare Tecnico di cui all'allegato B al Codice privacy.

Data breach: occorrono indicazioni per chiarire:

1) le ipotesi di violazione dei dati personali che presentano un rischio specifico e che, quindi, determinano l'obbligo di notifica all'Autorità (e, di converso, i casi che invece non determinano tale obbligo, ma solo quelli di documentazione e rendicontazione);

2) le ipotesi di violazione di dati personali suscettibili di presentare un rischio elevato, che determinano anche l'obbligo di comunicazione delle stesse all'interessato.

Valutazione di impatto privacy: il WP29 sta lavorando alle Linee Guida, per fornire indicazioni alle Autorità di controllo, affinché possano adottare:

1) l'elenco – obbligatorio – dei trattamenti soggetti a valutazione;

2) l'elenco – facoltativo - dei trattamenti non soggetti a valutazione.

L'auspicio è che gli elenchi vengano adottati il prima possibile e che l'Autorità adotti sul punto un approccio sostanziale, limitando l'adempimento ai casi in cui sussista un effettivo rischio per i diritti degli interessati, predisponendo *format* per supportare i Titolari nelle operazioni di valutazione ed esonerando le imprese più piccole.

Diritto alla portabilità dei dati: in primo luogo, occorre precisare quando il diritto alla portabilità dei dati trova applicazione *nel contesto della gestione del personale.* Le Linee Guida del WP29 sul punto rimangono molto generiche e rinviano alla valutazione caso per caso delle condizioni che legittimano l'esercizio del diritto alla portabilità, ferma restando l'esclusione dei trattamenti fondati sull'interesse legittimo e di quelli necessari per l'adempimento di obblighi legali in materia di lavoro.

In particolare, con riferimento alla portata del diritto alla portabilità in ambito lavoristico, sarebbe opportuno un chiarimento volto a escludervi i dati del lavoratore contenuti nelle schede di valutazione predisposte dal datore di lavoro. Tali informazioni, infatti, costituiscono *espressione del libero e soggettivo convincimento del valutatore* ovvero del *diritto alla libertà di pensiero del datore di lavoro* (v. Comunicato stampa del Garante privacy del 17 giugno 1999; Provvedimento del Garante privacy 5 dicembre 2001): il loro trattamento, quindi, è da inquadrare tra quelli finalizzati al perseguimento di un interesse legittimo, che lo stesso WP29 esclude dall'ambito di applicazione del diritto alla portabilità. Peraltro, la portabilità della scheda valutativa comporterebbe il rischio di diffondere informazioni aziendali di carattere riservato, che rafforza ulteriormente l'esigenza di una simile limitazione. Si pensi, ad esempio, a una valutazione positiva, con riferimenti al processo produttivo o ad altri dettagli dell'attività d'impresa, che il lavoratore presenta come referenza a un colloquio di lavoro: il nuovo esaminatore potrebbe apprendere elementi riservati e usarli impropriamente a danno dell'impresa.

Sempre con riferimento alla portata del diritto alla portabilità dei dati, sarebbe opportuno che l'Autorità fornisse indicazioni, anche a titolo esemplificativo, in merito ai trattamenti che, in ambito aziendale, sono esclusi poiché necessari all'*adempimento di un obbligo legale cui è soggetto il titolare del trattamento*.

Infine, appaiono opportune delle precisazioni con riferimento a:

1. i tempi entro i quali è esercitabile il diritto alla portabilità dei dati. Sul punto, andrebbe chiarito che l'esercizio del diritto è escluso una volta che il contratto sia cessato e il trattamento dei dati da parte del Titolare sia concluso;
2. i casi di rifiuto legittimo di una richiesta di portabilità, ferme restando le richieste di "carattere ripetitivo", espressamente menzionate dall'art. 12 co. 5 del GDPR;
3. i formati di dati portabili e le misure tecniche idonee per garantire la portabilità e la sicurezza dei dati, oltre a quelle specificamente individuate dal WP29.

Sanzioni: l'*accountability* si è tradotta, tra l'altro, in un irrigidimento dell'impianto sanzionatorio (il GDPR prevede massimi edittali fino al 4% del fatturato mondiale annuo). È fondamentale, soprattutto nella prima fase di operatività del nuovo regime, che l'Autorità adotti sul punto un approccio di cautela, privilegiando le ulteriori soluzioni previste dall'art. 83 del GDPR (avvertimenti, ammonimenti, ingiunzioni, limitazioni e divieti) e tenendo conto di tutti i criteri di applicazione e quantificazione della sanzione.