GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

DIPARTIMENTO REALTA' ECONOMICHE
E PRODUTTIVE

Roma, 18/5/2018
Prot. 15048/122644

Spett.le Confindustria
Viale dell'Astronomia 30
00144 Roma

c.a. Antonio Matonti
a.matonti@confindustria.it

Rif: DREP/CDA/122644/1
OGGETTO: richiesta di parere sulla designazione del responsabile del trattamento e sul modello di registro delle attività di trattamento.

Si fa riferimento alle Vs. comunicazioni del 12 dicembre 2017 e del 6 marzo 2018, con le quali, in vista dell'imminente applicazione del Regolamento Europeo n. 2016/679 – di seguito "RGPD", sono stati formulati alcuni quesiti in merito alle modalità di designazione del responsabile del trattamento ed è stato sottoposto a questa Autorità anche un modello di registro delle attività di trattamento (art. 30 del RGPD) da mettere a disposizione delle imprese associate.

In merito, nel considerare congiuntamente le suddette richieste in quanto relative a materie strettamente correlate, si formulano alcune prime osservazioni come di seguito sintetizzate.

Innanzitutto, va sottolineato che l'istituzione del registro delle attività di trattamento rappresenta un aspetto di particolare rilievo del nuovo quadro normativo europeo costituendo uno dei principali elementi di *accountability* del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, alla base di ogni attività di valutazione o analisi del rischio (v. Garante per la protezione dei dati personali, "Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali", pag. 26).

Per tali ragioni, il RGPD ne individua la natura in termini di obbligo di portata generale, ovvero di adempimento rivolto a tutti i titolari/responsabili del trattamento, prevedendo, al suo interno, un'unica eccezione per imprese (o organizzazioni) con meno di 250 dipendenti che non effettuino trattamenti c.d. "rischiosi" (ovvero trattamenti che presentino un rischio - anche non elevato- per i diritti e le libertà dell'interessato, non siano occasionali o includano categorie particolari di dati ai sensi degli artt. 9 e 10 del RGPD; v. art. 30, par. 5 del RGPD).

Su questo aspetto, con particolare riferimento all'esatta individuazione della platea dei soggetti destinatari della deroga sopra citata, il Gruppo ex art. 29 si è di recente espresso con un documento interpretativo (v. *Art. 29 WP*,

Piazza di Monte Citorio, 121 - 00186 Roma
Tel. +39 06 696771 - Fax +39 06 696773785
drep@garanteprivacy.it

Position Paper related to article 30(5), del 19 aprile 2018) che, nel confermare il carattere alternativo delle tre condizioni individuate dall'art. 30, par. 5 del RGPD, precisa, in particolare, che le organizzazioni con meno di 250 dipendenti non rientranti nella suddetta deroga in ragione dei trattamenti effettuati, potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle specifiche attività "rischiose" individuate ai sensi dell'art. 30, par. 5 del RGPD (es. ove il trattamento delle categorie particolari di dati ai sensi dell'art. 9 del RGPD si riferisca a quelli inerenti un solo lavoratore dipendente, il registro dovrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

Nel contesto sopra individuato e stante la portata tendenzialmente generale dell'obbligo di tenuta del registro (così come risultante dalla predetta interpretazione), il modello da Voi predisposto potrebbe rappresentare un'utile strumento da mettere a disposizione in particolare delle piccole e medie imprese (di seguito "PMI") soprattutto ove associato ad alcune linee guida di carattere operativo, che si traducano in un elemento di primo aiuto alle organizzazioni nell'ambito dei nuovi adempimenti imposti dal RGPD.

In tale ottica, appare condivisibile la Vs. proposta di "accompagnare" il modello di registro con un "Glossario" che ne agevoli la relativa compilazione, possibilmente in combinazione con alcune ulteriori indicazioni, di seguito esplicitate, volte a meglio definire la portata dell'obbligo medesimo e le modalità di implementazione dello stesso.

In primis con riferimento alle "*categorie di destinatari a cui i dati sono stati o saranno comunicati*" (art. 30, par. 1, lett. d) del RGPD), è opportuno chiarire che in tale sezione andranno indicati, anche semplicemente per categoria di appartenenza, non solo gli altri titolari cui i dati siano comunicati, ma anche gli eventuali responsabili del trattamento nominati dal titolare.

In particolare, in ordine alla figura del responsabile del trattamento occorre far presente che tale soggetto deve essere designato ai sensi dell'art. 28 del RGPD, ovvero con un contratto (o altro atto giuridico vincolante) il cui contenuto minimo è espressamente individuato dalla normativa di riferimento (v. nello specifico l'art. 28, par. 3 del RGPD). Sarà pertanto utile rammentare ai Vs. associati l'opportunità di valutare, alla luce del RGPD, i rapporti già in essere con eventuali soggetti esterni cui siano conferite attività di trattamento di dati personali, al fine sia di verificare la necessità di intervenire con la sopra menzionata designazione a responsabile del trattamento, ove non ancora effettuata, sia nell'ottica di apportare ai rapporti già in atto le necessarie integrazioni o modifiche, specialmente in materia di misure di sicurezza o designazione dei sub-responsabili.

Con specifico riguardo a questi ultimi, oltre a quanto già detto sopra in materia di obblighi di nomina e di verifica, appare utile rammentare che il titolare deve preventivamente autorizzare per iscritto il responsabile ove questi ricorra ad altri sub-responsabili e deve essere tempestivamente informato di

ogni eventuale modifica riguardante l'aggiunta o la sostituzione dei suddetti sub-responsabili (art. 28, paragrafi 2 e 4 del RGPD); ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate in tutto o in parte le attività di trattamento dei dati personali.

In merito all'ipotesi in cui le suddette attività di trasmissione dei dati ad altri soggetti integrino al contempo un'attività di trasferimento verso Paesi terzi, si fa presente che tale informazione dovrà essere riportata nell'apposita sezione del registro a ciò dedicata (v. art. 30, par. 1, lett. e) del RGPD), unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie adeguate" adottate ai sensi del capo V del RGPD. Tra queste, si rammenta che, con specifico riferimento al corrispondente paragrafo del Vs. "Glossario", andrebbe precisato che, in via residuale e solo a determinate condizioni (specificatamente individuate dal RGPD per singola situazione), è possibile trasferire, con riferimento per lo più a trattamenti di carattere meramente occasionale (v. c. 111 del RGPD), dati personali nell'ambito delle c.d. "deroghe" di cui all'art. 49, ricordando che quelle che nella prassi potrebbero essere di maggior utilizzabilità per le PMI, sono il consenso esplicito dell'interessato o l'esecuzione di un contratto concluso con il titolare o tra il titolare e un terzo a favore dell'interessato (v. art. 49, par. 1, lettere a), b) e c) del RGPD).

Quanto alle finalità del trattamento e alla descrizione delle categorie di interessati e di dati personali (art. 30, par. 1, lettere b) e c) del RGPD), la relativa sezione del Vs. modello di registro (nonché del "Glossario"), che comunque presenta un buon livello di dettaglio, potrebbe meglio precisare che, con particolare riferimento ai trattamenti posti in essere per perseguire il legittimo interesse del titolare o di un terzo (art. 6 par. 1, lett. f) del RGPD), devono essere esplicitate all'interno del registro, anche in vista del corrispondente obbligo informativo previsto in capo al titolare (art. 13, par. 1, lett. d, e art. 14, par. 2, lett. b, del RGPD), sia il legittimo interesse in concreto perseguito sia le garanzie adeguate ivi approntate, nonché, ove effettuata, l'eventuale valutazione d'impatto posta in essere (v. anche provv. del Garante del 22 febbraio 2018 – [doc web n. 8080493]).

Con riferimento ai termini di cancellazione (art. 30, par. 1, lett. f) del RGPD), potrebbe essere opportuno, soprattutto nell'ottica di fornire un concreto supporto alle PMI, provare ad individuare alcuni termini di cancellazione "tipizzabili" per tipologie di trattamento (es. in caso di rapporto contrattuale, 10 anni dall'ultima registrazione in ragione del generale obbligo di conservazione delle scritture contabili di cui all'art. 2220 del codice civile ecc.), possibilmente iniziando da quei trattamenti che, nell'ambito delle PMI, ricorrono con maggior frequenza (es. quelli che attengono alle c.d. "finalità amministrativo-contabili").

Infine, in materia di misure sicurezza, preso atto delle prime indicazioni fornite nel Vs. "Glossario", si coglie l'occasione per richiamare l'attenzione dei titolari/responsabili sulla circostanza che la lista da Voi fornita (così come quella di cui all'art. 32 del RGPD) è comunque una lista aperta e non esaustiva, essendo ad ogni modo rimessa al titolare e al responsabile la valutazione finale

relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere (v. anche "Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali", cit., pag. 27). Tale lista (o altre analoghe) ha di per sé un carattere dinamico (e non più statico come è stato per l'Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi.

Tanto premesso, rappresentando da ultimo che il quadro giuridico di riferimento non è stato ancora completato dal legislatore nazionale e che quindi, non appena esso sarà definito, sarà cura di questa Autorità fornire ogni utile ulteriore informazione agli operatori del settore, si ringrazia per l'attenzione prestata all'attività istituzionale di questa Autorità.

Il dirigente
(dott. Daniele De Paoli)