mise.AOO_AG.REGISTRO UFFICIALE.U.0002663.28-01-2020

Il Ministro dello Sviluppo Economico

VISTO il decreto legislativo 30 marzo 2001, n. 165 e successive modificazioni, recante *"Norme generali sull' ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";*

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante il "*Codice in materia di protezione dei dati personali*";

VISTO il decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni, recante *"Codice dell'amministrazione digitale";*

VISTO il 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, che abroga la direttiva 95/46/CE, divenuto direttamente applicabile il 25 maggio 2018;

VISTA la legge di delegazione europea del 25 ottobre 2017, n. 163;

VISTO il decreto legislativo 10 agosto 2018, n. 101 (in vigore dal 19 settembre 2018), recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento(UE) 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati",* che interviene a modificare il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

VISTO il decreto del Presidente della Repubblica 28 novembre 2008, n. 198, recante "*Regolamento di definizione della struttura degli uffici di diretta collaborazione del Ministero dello Sviluppo Economico*";

VISTO il decreto del Presidente del Consiglio dei Ministri 19 giugno 2019 n. 93, pubblicato in G.U 21 agosto 2019, n. 195, con cui è stato adottato il "*Regolamento concernente l'organizzazione del Ministero dello sviluppo economico, ai sensi dell'articolo 4-bis del decreto-legge 12 luglio 2018, n. 86, convertito, con modificazioni, dalla legge 9 agosto 2018, n. 97*";

VISTO il decreto del Presidente del Consiglio dei Ministri 12 dicembre 2019, di modifica del DPCM 19 giugno 2019 n. 93, adottato a seguito dell'entrata in vigore del decreto-legge n. 104/2019 convertito con modificazioni, dalla legge 18 novembre 2019, n. 132;

PP

VISTO il dPCM 29 ottobre 2019, registrato dalla Corte dei Conti in data 26 novembre 2019 Reg. prev. 1041 con cui si è proceduto alla nomina del Responsabile della protezione dei dati – RPD (Data Protection Officer - DPO) per il Ministero dello sviluppo economico;

VISTO il decreto ministeriale 14 gennaio 2020 relativo all'individuazione degli uffici dirigenziali di livello non generale del Ministero dello sviluppo economico;

EMANA
la seguente

DIRETTIVA PER LA INDIVIDUAZIONE DEI SOGGETTI ATTRAVERSO I QUALI IL MINISTERO DELLO SVILUPPO ECONOMICO ESERCITA LE FUNZIONI DI TITOLARE DEL TRATTAMENTO, AI SENSI DEL REGOLAMENTO (UE) 2016/679, RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÈ ALLA LIBERA CIRCOLAZIONE DI TALI DATI.

Articolo 1
(Premesse)

1. La presente direttiva individua i soggetti attraverso i quali il Ministero dello sviluppo economico esercita le funzioni di Titolare del trattamento dei dati personali nel rispetto dei principi di proporzionalità, pertinenza e non eccedenza, ai sensi della normativa prevista dal Regolamento (UE) 2016/679 (di seguito, "Regolamento"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
2. Il Ministero si impegna ad armonizzare l'assetto organizzativo con lo sviluppo del quadro normativo relativo alla tutela dei dati personali delle persone fisiche contemperando l'esigenza, privata, di protezione di tali dati con l'esigenza, pubblica, di trasparenza.
3. Il presente atto individua i soggetti attraverso i quali il Ministero dello sviluppo economico esercita le funzioni di Titolare del trattamento dei dati, in coerenza con l'attuale struttura organizzativa.

Articolo 2
(Definizioni in materia di trattamento dei dati personali)

Al fine di fornire indicazioni in ordine al trattamento di dati personali, si riportano di seguito

PP

alcune definizioni normative contenute nel Regolamento:

dato personale: *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*;

trattamento: *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione* di dati personali;

profilazione: *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*;

pseudonimizzazione: *il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;*

titolare del trattamento (*Data controller*): *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*;

responsabile del trattamento: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*;

PP

interessato: *la persona fisica cui si riferiscono i dati personali oggetto del trattamento*;

Articolo 3

(*Principi applicabili al trattamento dei dati*)

Ai sensi dell'art. 5 del Regolamento, i principi alla base del corretto trattamento dei dati personali sono i seguenti:

a) **Liceità, correttezza e trasparenza**: il trattamento dei dati personali deve avvenire in modo lecito, corretto e trasparente, deve essere consentito da leggi e/o regolamenti e deve essere esente da errori o difetti. Gli interessati coinvolti devono ricevere informazioni trasparenti sull'utilizzo che sarà fatto dei loro dati.
b) **Limitazione della finalità**: la finalità del trattamento ovvero la motivazione che è alla base del trattamento dei dati personali deve essere legittima e deve essere determinata ed esplicitata con chiarezza. Inoltre le modalità di trattamento devono essere compatibili con la finalità dichiarata; non è possibile utilizzare i dati per scopi ulteriori e diversi.
c) **Minimizzazione dei dati**: i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario al raggiungimento della finalità dichiarata. Non è permesso raccogliere o conservare informazioni aggiuntive o superflue rispetto alla finalità dichiarata.
d) **Esattezza**: i dati su cui si opera devono essere esatti. I dati inesatti devono essere aggiornati, rettificati o aggiornati nel loro "ciclo di vita" all'interno dell'organizzazione.
e) **Limitazione della conservazione**: i dati personali possono essere conservati solo per il tempo necessario a consentire l'identificazione degli interessati cioè per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati sono trattati. Per ogni trattamento è obbligatorio definire i tempi di conservazione dei dati personali e attenervisi.
f) **Integrità e riservatezza**: il trattamento dei dati deve essere protetto da misure tecniche ed organizzative adeguate a garantire la sicurezza e la protezione al fine di scongiurare trattamenti non autorizzati o illeciti e per evitare che i dati siano distrutti o cancellati, anche per errore.

Articolo 4

(Principio di accountability del Titolare ovvero principio di responsabilizzazione)

1. Il Titolare del trattamento deve osservare i principi indicati nell'art. 3 e deve essere in grado di

provare di averli rispettati lungo tutta la filiera del trattamento.

2. La protezione e la sicurezza dei dati personali devono essere garantite:
   a) al momento della progettazione del trattamento (*by design*);
   b) per tutta la durata del trattamento (*by default*).

3. A tale fine il Titolare del trattamento deve adottare misure tecniche ed organizzative dirette a garantire che:
   a) per ciascuna finalità di trattamento siano raccolte e trattate solo le informazioni personali strettamente necessarie (*principio di minimizzazione*);
   b) il trattamento effettuato non ecceda le finalità dichiarate e non prosegua per un tempo più lungo di quello necessario per il raggiungimento della specifica finalità;
   c) i dati personali allo scadere del periodo di conservazione definito dal Titolare siano eliminati;
   d) i dati siano trattati solo da personale autorizzato in virtù dei compiti;
   e) sia inibita la possibilità di accedere indiscriminatamente agli archivi o di estrarre dati personali in modo massivo da una banca dati senza l'intervento e l'autorizzazione preventiva di un responsabile.

Articolo 5

(*Soggetti che esercitano le funzioni di Titolare del trattamento dei dati personali*)

1. Il Titolare del trattamento dei dati personali è il Ministero dello sviluppo economico.

2. In conformità alla struttura organizzativa del Ministero dello sviluppo economico i soggetti attraverso i quali il Ministero esercita le funzioni di Titolare del trattamento dei dati personali, ciascuno nel rispettivo ambito di competenza, sono: il Capo di Gabinetto; il Segretario Generale; i Direttori generali; i Titolari di incarichi di livello dirigenziale generale e il Titolare dell'Organismo indipendente di valutazione della *performance* del Ministero dello sviluppo economico.

Articolo 6

(*Liceità del trattamento*)

Il trattamento dei dati personali è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

   a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

PP

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Articolo 7

(Diritti dell'interessato)

1. L'interessato ha diritto di essere informato del trattamento, di accedere ai propri dati, di ottenerne la rettifica o la cancellazione (*diritto all' "oblio"*).
2. L'interessato ha diritto alla limitazione del trattamento dei propri dati, presentando richiesta motivata per ottenerne, per un periodo di tempo, il blocco e ha diritto alla portabilità dei dati, ovvero può chiedere al Titolare di trasmettere direttamente i propri dati personali ad un altro Titolare da lui indicato, se la tecnica lo consente.
3. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano. Quando l'interessato si oppone, il Titolare si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
4. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione. In tal caso, i dati personali non potranno più essere oggetto di trattamento per tali finalità.

Articolo 8

(*Analisi del rischio e valutazione d'impatto*)

1. Il Titolare del trattamento ha l'obbligo di effettuare un'analisi del rischio e di condurre una valutazione preliminare d'impatto (*DPIA –Data Protection Impact Assessment*) della protezione dei

dati quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'ambito di applicazione, il contesto e le finalità del trattamento.

2. L'autorità di controllo competente, deve essere consultata quando una valutazione di impatto "*indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*" oppure, a prescindere dall'adozione di tali eventuali misure, "*il tipo di trattamento, in particolare se utilizza tecnologie, procedure o meccanismi nuovi, presenta un rischio elevato per i diritti e le libertà degli interessati*".

Articolo 9

(*Compiti del Titolare del Trattamento*)

1. Il Titolare, ai sensi dell'art. 24 del Regolamento, è responsabile dell'intero ciclo di vita dei dati che gli sono affidati dagli interessati, dal momento della raccolta al momento della cancellazione.

2. Il Titolare è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali.

Costituiscono obblighi del Titolare del trattamento:

a) notificare al Garante della protezione dei dati personali le violazioni dei dati personali (cd. *data breach),* provvedere alla comunicazione della violazione agli interessati, ai sensi degli artt.33 e 34 del Regolamento e darne informativa al Segretario generale e al Responsabile della protezione dati;
b) adottare misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (*privacy by design*) e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente;
c) osservare il dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
d) designare il Responsabile del trattamento a cui affidare mansioni di elevata professionalità, in fase di gestione dei dati personali;
e) nominare un referente del Responsabile della protezione dati, nell'ambito della propria struttura, che agevoli le comunicazioni in materia di protezione dati, facilitandone gli adempimenti conseguenti e attuandone le indicazioni ricevute;
f) effettuare l'analisi del rischio e la valutazione preliminare d'impatto (cd. *DPIA)* di cui all'art. 35 del Regolamento;

g) tenere e aggiornare il registro di trattamenti;
h) garantire la formazione del personale;
i) documentare le violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

3. Quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. In quanto tali, determinano in modo trasparente, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento mediante un accordo formale che deve "riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati". L'accordo deve essere messo per iscritto o in un formato elettronico comparabile e attendibile e deve contenere indicazioni circa:

a) la natura e la finalità del trattamento;
b) le categorie di dati personali trattati e le categorie di interessi coinvolti;
c) la durata del trattamento.

4. Coloro che esercitano le funzioni di Titolare del trattamento dovranno compiere i controlli necessari a verificare la conformità alla normativa sul trattamento dei dati personali da parte dei Responsabili del trattamento, sincerandosi che questi ultimi si limitino ai trattamenti di dati personali espressamente previsti nel contratto o altro atto giuridico di cui sopra.

Articolo 10

(*Responsabile della Protezione dei dati*)

1. Il Ministro nomina il Responsabile della protezione dei dati - RPD (*Data Protection Officer*-DPO) tra i soggetti in possesso dei requisiti professionali di cui all'art. 37 del Regolamento.

2. Il Responsabile Protezione Dati è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

a) informare e fornire consulenza in merito alla protezione dei dati personali a tutta l'organizzazione nella quale opera, promuovendo la conoscenza di leggi e regolamenti;
b) sorvegliare l'osservanza delle norme e delle politiche dell'organizzazione sulla protezione dei dati personali, vigilando sull'attribuzione delle responsabilità, e sulla formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire pareri, se richiesto, in merito alla valutazione preliminare d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto con l'autorità di controllo per ogni questione relativa al trattamento dei dati personali.

3. Il Ministero dello sviluppo economico si impegna a:
   a) mettere a disposizione del Responsabile Protezione Dati una struttura di supporto, assegnando le risorse professionali necessarie al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate;
   b) garantire che il Responsabile Protezione Dati eserciti le proprie funzioni in autonomia e indipendenza come previsto dall'art. 38 del Regolamento.

4. Il soggetto designato e i dati di contatto del Responsabile Protezione Dati sono resi disponibili sulla intranet e sul sito istituzionale del Ministero dello sviluppo economico e comunicati al Garante per la protezione dei dati personali.

Articolo 11

(Compiti del Responsabile del Trattamento)

1. La funzione di Responsabile del trattamento discende da un contratto o altro atto giuridico, sottoscritto dal Titolare del trattamento o da chi ne esercita le funzioni. Il Responsabile del trattamento tratta i dati personali in applicazione di quanto espressamente previsto nel contratto o in altro atto giuridico, in ordine a:
   a) materia disciplinata e durata del trattamento;
   b) natura e finalità del trattamento;
   c) tipo di dati personali;
   d) categorie di interessati;
   e) obblighi e diritti del Titolare del trattamento.

2. Il contratto o altro atto giuridico deve prevedere, ai sensi dell'art. 28 del Regolamento, che il Responsabile del trattamento:
   a) tratti i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
   b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

AA

c) adotti tutte le misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio (es. pseudonimizzazione e cifratura dei dati personali);
d) acquisisca la preventiva autorizzazione scritta, specifica o generale del Titolare del trattamento per ricorrere a un altro Responsabile del trattamento (sub-responsabile);
e) assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste di esercizio dei diritti degli interessati;
f) assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione;
g) su scelta del Titolare del trattamento cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
h) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

3. Il Responsabile del trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Art. 12

(Designati al trattamento)

1. I Titolari dei trattamenti possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, dirigenti di seconda fascia e/o funzionari espressamente designati, che operano sotto la loro autorità, in ossequio all'art. *2-quaterdecies* del D.lgs. 196/2003, introdotto dal D.lgs. 101/2018. A costoro sono attribuite, alla luce del principio di responsabilizzazione (*accountability)* funzioni di coordinamento e attuazione degli adempimenti tecnico-organizzativi in materia di trattamento e protezione dei dati personali, all'interno di strutture complesse e/o articolate territorialmente.
2. I soggetti di cui al comma 1 sono nominati con decreto direttoriale.

RP

Art. 13

(Autorizzati al trattamento)

1. I Titolari dei trattamenti individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
Gli autorizzati, ossia coloro che sono preposti alle operazioni di trattamento di dati personali e che, in ragione del proprio Ufficio, sevizio o attività, sono legittimati ad accedere alle informazioni personali contenute negli archivi, banche dati, atti o documenti del Ministero, sono individuati e istruiti dai soggetti che esercitano le funzioni di Titolare del trattamento, operando sotto la loro diretta autorità.
2. In assenza di una formale designazione, i dipendenti che verranno a conoscenza di dati personali, saranno da considerarsi quali soggetti terzi rispetto al Titolare del trattamento.

Articolo 14

(*Registri delle attività di trattamento*)

1. Il Segretario Generale, nell'esercizio delle sue funzioni istituzionali di coordinamento, avvalendosi del supporto tecnico-operativo del Responsabile Protezione Dati e del supporto informatico della Direzione per le risorse l'organizzazione i sistemi informativi e il bilancio, indica agli Uffici del Ministero dello sviluppo economico, con proprio atto, le modalità operative per l'organizzazione del Registro delle attività di trattamento, ai sensi dell'art. 30 del Regolamento.
2. Ogni Titolare del trattamento e, ove applicabile, il suo rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del Titolare del trattamento e del Responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un' organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione e la documentazione delle garanzie adeguate relativamente alla protezione dei dati personali;

pp

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative implementate per la sicurezza dei trattamenti.

3. Ogni Responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento, contenente:

a) il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del Rappresentante del titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso organizzazioni internazionali o verso paesi situati fuori dai confini europei (che devono essere indicati) e la documentazione delle garanzie adeguate in materia di protezione dei dati personali;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative implementate per la sicurezza dei trattamenti

4. I registri di cui ai paragrafi 2 e 3 sono tenuti in forma scritta, anche in formato elettronico.Su richiesta, il Titolare del trattamento o il Responsabile del trattamento e, ove applicabile, il rappresentante del Titolare del trattamento o del Responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Articolo 15

(*Informative e gestione delle richieste degli interessati*)

1. È compito dei soggetti che esercitano le funzioni di Titolare del trattamento rendere le informative agli interessati, in tutti i casi in cui ciò si renda necessario, previa verifica della loro corretta predisposizione e del loro costante aggiornamento.

2. In relazione a possibili istanze avanzate dagli interessati al trattamento, gli esercenti le funzioni di titolare avranno cura di adottare tutte le misure tecniche ed organizzative appropriate per garantire ai medesimi interessati l'esercizio dei propri diritti riconosciutigli dal Regolamento e da specifiche disposizioni normative

Articolo 16

(Violazioni di dati personali -Data breach)

1. La violazione dei dati personali consiste in una violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
2. Chiunque venga a conoscenza di una violazione dei dati personali è tenuto a segnalarla, per il tramite del proprio superiore gerarchico, al soggetto che esercita le funzioni di Titolare del trattamento, il quale deve provvedere tempestivamente ai sensi del presente articolo.
3. Il Responsabile del trattamento informa il soggetto che esercita le funzioni di Titolare del trattamento tempestivamente, dopo essere venuto a conoscenza della violazione.
4. Il soggetto che esercita le funzioni di Titolare del trattamento notifica la violazione dei dati personali al Garante della protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sia venuto a conoscenza, a meno che risulti improbabile che la violazione determini un rischio per la tutela dei diritti e delle libertà delle persone fisiche. La notifica deve contenere almeno gli elementi indicati all'art. 33, comma 3 del Regolamento.
5. Qualora la notifica al Garante della protezione dei dati personali venga effettuata oltre le 72 ore, deve essere corredata dei motivi del ritardo.
6. Se la gestione dell'infrastruttura tecnica è affidata ad un terzo, il contratto tra Titolare e Responsabile deve vincolare quest'ultimo a comunicazioni tempestive e trasparenti in merito agli eventi di violazione subiti, in modo che il Titolare possa adempiere ai propri obblighi nei tempi e nei modi previsti.
7. Il Titolare ha altresì l'obbligo di informare al più presto gli interessati se i loro diritti o la loro libertà rischiano di essere lesi in modo significativo. La comunicazione agli interessati non è richiesta nel caso in cui:
   a) le misure tecniche ed organizzative disponibili prima della violazione hanno reso i dati personali incomprensibili alle persone non autorizzate ad accedervi (ad esempio, i dati sono crittografati)
   b) a seguito della violazione, ha adottato misure che non rendono possibile il verificarsi di un rischio elevato per i diritti e le libertà dell'interessato.
8. Il Titolare deve attivarsi per ogni segnalazione ricevuta, tracciarla in un apposito registro e documentarne l'evoluzione, registrando l'esito delle indagini compiute e le azioni eventualmente intraprese per limitarne le conseguenze.

9. Le segnalazioni e le notifiche dei casi di violazione dei dati personali sono comunicate dai Titolari del trattamento al Segretario generale e al Responsabile Protezione Dati.
10. Ulteriori, specifiche modalità operative ed organizzative per la segnalazione e la gestione dei casi di violazione dei dati personali possono essere supportate da soluzioni applicative messe a disposizione dalla Direzione per le risorse, l'organizzazione, i sistemi informativi e il bilancio.

Articolo 17

(*Principi di gestione e aggiornamento della documentazione*)

La documentazione relativa al trattamento dei dati personali deve essere periodicamente controllata per verificare la necessità di un suo aggiornamento determinato da una delle seguenti motivazioni:

a) modifiche normative che devono essere recepite;
b) introduzione di nuovi processi, servizi o prodotti,
c) variazioni a processi, servizi o prodotti esistenti, anche dovute all'insorgenza di nuovi rischi o a modifiche nella loro valutazione.

Articolo 18

(*Formazione del personale*)

La Direzione generale per le risorse, l'organizzazione, i sistemi informativi e il bilancio, assicura la programmazione e l'organizzazione delle attività di formazione del personale per la corretta applicazione delle disposizioni in materia di trattamento di dati personali, tramite il coordinamento del Responsabile Protezione Dati.

Roma, 28 GEN. 2020

IL MINISTRO

On. Stefano Patuanelli