D.D.G. n. 915

REPUBBLICA ITALIANA
REGIONE SICILIANA

Assessorato regionale delle Autonomie Locali e della Funzione Pubblica
Dipartimento regionale della Funzione Pubblica e del Personale

Nomina del Responsabile esterno del trattamento dei dati personali relativi alla Progressione Economica Orizzontale del Personale del Comparto non dirigenziale della Regione Siciliana e degli Enti di cui all'articolo 1 della L.R. 15 maggio 2000, n.10

IL DIRIGENTE GENERALE

Visto lo Statuto della Regione Siciliana;

Viste la legge regionale 29 dicembre 1962, n. 28 e la legge regionale 10 aprile 1978, n. 2;

Visto il D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";

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 e che abroga la direttiva 95/46/CE" e, in particolare, l'art. 27 "Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione" e l'art. 28 "Responsabile del trattamento", commi 2 e 4;

Visto il D. Lgs. 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/4/2016";

Vista la deliberazione della Giunta regionale di Governo 28 maggio 2018, n. 203 "Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 – Nomina del Responsabile per la protezione dei dati";

Vista la deliberazione della Giunta Regionale di Governo 29 novembre 2018 n. 483, "Regolamento UE 2016/679 – Adozione delle prime istruzioni organizzative e tecniche per il trattamento dei dati personali, di una procedura di risposta e di un questionario di autovalutazione"

Visto il D.P. n. 02/Area 1/S.G. del 04 gennaio 2021 con il quale l'Avv. Marco Zambuto è stato nominato Assessore regionale delle Autonomie Locali e della Funzione Pubblica;

Visto il D.P. Reg. n. 569 del 12 giugno 2018, con il quale è stato nominato il Responsabile della protezione dei dati per la Regione Siciliana;

Visto il D.P. Reg. n. 2804 del 19 giugno 2019, con il quale alla Dr. ssa Carmela Madonia è stato conferito l'incarico di Dirigente Generale del Dipartimento regionale della Funzione Pubblica e del Personale

Vista la nota n. 36313 del 13/04/2021, con cui l'Assessore Marco Zambuto, nella qualità di Titolare del trattamento, conferma il D.A. n. 2896 del 25 giugno 2020, con il quale l'Assessore On. le Bernardette Grasso aveva conferito al Dirigente Generale del suddetto Dipartimento regionale, l'incarico di Responsabile dei trattamenti di dati personali che rientrano tra le competenze dello stesso Dipartimento, con facoltà di ricorrere ad altri

soggetti responsabili ai quali affidare in tutto o in parte il trattamento dei dati, ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016;

Visto il D.D.G. n. 7713 del 27 dicembre 2018 del Dipartimento Regionale dell'Istruzione e della Formazione, con il quale è stata approvata la Convenzione tra la Regione Siciliana - Dipartimento regionale dell'Istruzione e della Formazione - ed il Formez PA, stipulata in data 5 dicembre 2018, avente ad oggetto il servizio finalizzato alla realizzazione del progetto denominato "Nuovi percorsi di sviluppo della Capacità amministrativa della Regione Siciliana";

Vista la nota n. 61415 del 09/07/2020, con cui il Dipartimento della Funzione Pubblica e del Personale chiedeva di realizzare un'attività formativa per il potenziamento delle competenze del comparto non dirigenziale del personale regionale, nell'ambito delle iniziative ricomprese nella suddetta convenzione;

Visto il riscontro della suddetta nota da parte del Formez PA, con cui si confermava la disponibilità ad effettuare le verifiche per incardinare questa attività nell'ambito della Linea 2.2. Azione 1 - Sviluppo delle competenze del progetto "Nuovi percorsi", previa attivazione di procedure per l'acquisizione dei quesiti nonchè per la successiva somministrazione attraverso una piattaforma dedicata;

Considerato che qualora un soggetto esterno sia chiamato ad eseguire una o più attività di trattamento di dati personali per conto del Titolare, è necessario nominarlo Responsabile esterno del trattamento dei dati ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016, attribuendogli le relative competenze;

Considerato che il Responsabile esterno del trattamento dei dati, è obbligato ad adottare le misure di sicurezza di natura fisica, logica, tecnica e organizzativa idonee a garantire un livello di sicurezza adeguato al rischio e conformi alla normativa vigente e alle istruzioni fornite dall'Amministrazione;

Ritenuto di dover individuare, ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016, la società Formez PA - Centro servizi, assistenza, studi e formazione per l'ammodernamento delle P.A. (di seguito denominato "Formez PA"), con sede legale in Roma, Viale Marx n. 15 - CF: 80048080636, P.IVA 06416011002, quale Responsabile esterno del trattamento dei dati personali relativamente alle procedure legate all'attribuzione della PEO ed affidate al Formez PA, nell'ambito della Convenzione "Nuovi percorsi di sviluppo della Capacità amministrativa della Regione Siciliana";

DECRETA

Art. 1 – Nomina

1. Ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016, la società Formez PA con sede legale in Roma, Viale Marx n. 15 - CF: 80048080636, P.IVA 06416011002, è individuata quale Responsabile esterno del trattamento dei dati personali relativamente a tutte le procedure legate all'attribuzione della PEO ed affidate alla stessa nell'ambito della Convenzione "Nuovi percorsi di sviluppo della Capacità amministrativa della Regione Siciliana", relativamente alle procedure legate all'attribuzione della PEO ed affidate al Formez PA, di competenza dell'Assessorato regionale delle Autonomie locali e della Funzione pubblica - Dipartimento regionale della Funzione Pubblica e del Personale. (nel seguito

"Amministrazione"), nell'ambito della suddetta Convenzione con la Società stessa (nel seguito "Convenzione").

2. Il Responsabile esterno ha facoltà di designare sub-Responsabili del trattamento le società o i soggetti subappaltanti, previa comunicazione scritta da parte del Formez e salvo diverso avviso all'Assessorato regionale delle Autonomie Locali e della Funzione Pubblica, nella qualità di Titolare del trattamento dei dati, che può comunicare la propria opposizione per iscritto entro 10 giorni dalla notifica da parte del Responsabile esterno.
3. Il Responsabile esterno effettua il trattamento dei dati di cui all'allegato "A" al presente decreto nei limiti e nel rispetto delle finalità per cui sono stati raccolti. La nomina di Responsabile esterno ha validità dalla data di inizio operatività dell'Incarico ed è valida fino alla vigenza della stessa, o fino alla revoca anticipata per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione dell'Incarico o alla revoca, il Responsabile esterno dovrà mantenere la massima riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

Art. 2- Obblighi

1. Il Responsabile esterno ha facoltà, nell'ambito dell'esecuzione della Convenzione, di procedere alla nomina degli autorizzati al trattamento dei dati personali, mediante apposito atto di designazione. Per autorizzato si intende qualsiasi unità di personale interna alla Società, che sia autorizzata al trattamento dei dati personali, secondo le direttive e istruzioni impartite dalla Società stessa. Il Responsabile esterno fornisce all'Amministrazione l'elenco degli autorizzati.
2. Il Responsabile esterno, nell'ambito dell'esecuzione della Convenzione, ha l'obbligo di mettere in atto le misure di sicurezza di natura fisica, logica, tecnica e organizzativa idonee a garantire un livello di sicurezza adeguato al rischio e conformi alla normativa vigente, tenendo conto delle finalità perseguite, del contesto e delle specifiche circostanze in cui avviene il trattamento, nonché della tecnologia applicabile e dei costi di attuazione.
3. Il Responsabile esterno si deve attenere alle misure di sicurezza indicate dall'Amministrazione, di cui all'Allegato "B" al presente decreto, nonché di quelle specificate nella Convenzione e nei relativi allegati e da ogni ulteriore comunicazione in merito.
4. Il Responsabile esterno ha l'onere di informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione degli ulteriori sub-Responsabili. Il Titolare, avrà il diritto di opporsi a tali modifiche, comunicando la propria opposizione per iscritto entro 10 giorni dalla notifica da parte del Responsabile esterno. Il Responsabile esterno non ricorrerà ai sub-Responsabili, nei cui confronti il Titolare abbia manifestato la propria opposizione. Resta inteso che, in mancanza di opposizione, la modifica si intenderà accettata. Il Responsabile esterno impone al sub-Responsabile con apposito atto, gli stessi obblighi in materia di protezione dei dati che sono posti a suo carico in forza del presente decreto e vigila sul loro rispetto. Il Responsabile esterno rimarrà direttamente responsabile nei confronti del Titolare in ordine alle azioni ed alle omissioni dei propri sub-Responsabili ed ha l'onere di assicurare che il sub-Responsabile presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE 2016/679 del 27 aprile 2016.

Art. 3- Oneri e Responsabilità

1. Il Responsabile esterno assiste il Titolare in tutte le operazioni di sua competenza, inclusa quella di fornire risposta alla richiesta di esercizio dei diritti degli interessati, e ha l'onere di svolgere compiti di direzione e coordinamento sul corretto trattamento dei dati personali.
2. Il Responsabile esterno ha, altresì, l'onere di:
   a. mettere in atto misure tecniche e organizzative atte a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali per conto del Titolare è effettuato in conformità al Regolamento UE 2016/679 del 27 aprile 2016;
   b. adottare misure tecniche e organizzative idonee a garantire la sicurezza dei locali e delle postazioni di lavoro;
   c. fornire ai propri dipendenti e collaboratori autorizzati a trattare i dati personali le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività;
   d. predisporre ed aggiornare sistematicamente il proprio registro delle attività di trattamento dei dati personali trattati per conto del Titolare ed assistere il Titolare nell'aggiornamento del suo registro delle categorie di trattamento e il Dipartimento regionale della Funzione Pubblica e del Personale dell'Assessorato regionale delle Autonomie Locali e della Funzione Pubblica nell'aggiornamento del registro delle categorie di attività di trattamento;
   e. cooperare, su richiesta del Titolare, con il Garante della protezione dei dati personali (nel seguito "Autorità Garante") nell'esecuzione dei suoi compiti;
   f. fornire assistenza al Titolare per la gestione del consenso degli interessati al trattamento dei dati personali;
   g. fornire assistenza al Titolare per informare in maniera trasparente gli interessati sulla modalità di gestione e di protezione dei relativi dati personali trattati;
   h. fornire assistenza al Titolare per la gestione le richieste degli interessati sui propri dati personali trattati per conto del titolare;
   i. fornire assistenza al Titolare per l'analisi del rischio sui dati personali trattati;
   j. fornire assistenza al Titolare per la valutazione d'impatto dell'eventuale uso di nuove tecnologie sulla sicurezza dei dati personali trattati (*data protection impact assessment* o DPIA o VIP);
   k. comunicare al Titolare i dati di contatto del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE 2016/679 del 27 aprile 2016; il Responsabile esterno collabora e si tiene in costante contatto con il Responsabile della protezione dei dati della Regione Siciliana.
   l. collaborare con il Titolare e con il Responsabile della protezione dei dati della Regione Siciliana nell'attuazione delle ispezioni interne organizzative e tecniche volte alla verifica dell'attuazione di misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE 2016/679 del 27 aprile 2016;
   m. comunicare i luoghi dove sono memorizzati i dati, le loro copie e i sistemi che li trattano, e impegnarsi a non trasferirli in paese terzo rispetto la Unione europea;
   n. fornire assistenza al Titolare nell'aggiornamento della informativa da rendere agli interessati ai sensi degli art. 13 e 14 del Regolamento UE 2016/679 del 27 aprile 2016 in merito al trattamento in argomento;
   o. rendere disponibili tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dal Regolamento UE 2016/679 del 27 aprile 2016;

p. ove risulti che le misure adottate dal Responsabile esterno o da un sub-Responsabile non siano idonee ad assicurare l'applicazione del Regolamento UE 2016/679 del 27 aprile 2016 o che siano non siano correttamente applicate, adottare e far adottare al sub-Responsabile tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato dal Titolare. In caso di mancato adeguamento, l'Amministrazione potrà, in ragione della gravità della condotta e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il Contratto con il Responsabile esterno ed escutere l'eventuale garanzia prestata, salvo il risarcimento del maggior danno.

3. Il Responsabile esterno ha l'obbligo di informare il Titolare (inviando una comunicazione a mezzo PEC), senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne è venuto a conoscenza, di ogni violazione della sicurezza (*data breach*) che comporti 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, ed a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi, sullo stesso gravanti, di notifica delle suddette violazioni all'Autorità Garante ai sensi dell'art. 33 del Regolamento UE 2016/679 del 27 aprile 2016 o di comunicazione della stessa agli interessati ai sensi dell'art. 34 dello stesso Regolamento. Inoltre ha l'obbligo di comunicare le prime misure organizzative e tecniche adottate per porre rimedio alla violazione dei dati personali e per minimizzare gli effetti negativi e di proporre al Titolare l'adozione di ulteriori misure di sicurezza non immediatamente attuabili. Il Responsabile esterno fornisce al Titolare tutto il necessario supporto e la collaborazione per il riscontro alle richieste di informazioni aggiuntive da parte dell'Autorità Garante.
4. Il Responsabile esterno sarà responsabile per i danni conseguenti a inadempimenti o inosservanze delle istruzioni di cui all'Allegato B al presente provvedimento o di quelle successive eventualmente trasmesse per iscritto dall'Amministrazione.
5. Il Responsabile esterno, alla scadenza della Convenzione o, comunque, in caso di cessazione – per qualunque causa – dell'efficacia del presente atto di nomina, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario che preveda la conservazione dei dati personali, sarà tenuto ad interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, a scelta del Titolare, all'immediata restituzione allo stesso dei dati personali oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente un'attestazione scritta che presso lo stesso Responsabile esterno non ne esiste alcuna copia. Il Responsabile esterno fornisce assicurazione che allo stesso comportamento si sono adeguati i sub-Responsabili dallo stesso nominati. In caso di richiesta scritta del Titolare, il Responsabile esterno è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione dei dati.

Il presente decreto sarà pubblicato sul sito web del Dipartimento regionale della Funzione Pubblica e del Personale.

Palermo, 16/04/2021

Il Dirigente Reggente del Servizio
Emanuele Nicolosi

Firmato digitalmente da EMANUELE NICOLOSI
Data: 2021.04.16 08:26:45 +02'00'

Il Dirigente Generale
C. Madonia

CARMELA MADONIA

Firmato digitalmente da CARMELA MADONIA
Data: 2021.04.16 10:31:42 +02'00'

Allegato A

Titolare		*Assessorato regionale delle Autonomie Locali e della Funzione Pubblica e del Personale*					
N.	**Denominazione del trattamento**	**Finalità del trattamento**	**Categorie di interessati**	**Categoria dati personali**	**Durata del trattamento**	**Responsabile del Trattamento**	**Nella qualità di**
1	Gestione del personale dell'Amministrazione, necessaria ai fini della Progressione Economica Orizzontale della Regione siciliana	Attività istituzionale legata alla gestione del contratto di lavoro	Personale interno dell'amministrazione	Dati personali di identificazione e sede di servizio	24 mesi dal termine della chiusura delle procedure, salvo diverse esigenze derivanti da obblighi di legge.	Formez PA	Responsabile del trattamento esterno

MISURE DI SICUREZZA

Per garantire la sicurezza dei dati, il Responsabile esterno rivede regolarmente lo stato dell'arte delle tecnologie di sicurezza e le misure organizzative. Ciò include la determinazione di scenari di danno tipici, le esigenze di sicurezza e i livelli di sicurezza corrispondenti che ne derivano per diversi tipi di dati personali, raggruppati in categorie di possibili danni, l'esecuzione di valutazioni del rischio, la nomina di un Amministratore di sistema, l'adozione di politiche di gestione e di accesso ai dati personali. Inoltre, vengono effettuate verifiche di vulnerabilità dedicate per analizzare, esaminare e valutare regolarmente l'efficacia delle misure tecniche e organizzative che devono garantire la sicurezza del trattamento.

I seguenti aspetti disciplinano l'attuazione di misure tecniche e organizzative appropriate:

1. *Backup* dei dati

Per evitare perdite, il Responsabile esterno definisce idonee procedure affinché i dati vengono regolarmente sottoposti a *backup* veicolati dalle procedure di sicurezza IT e per la verifica dell'efficacia delle copie di sicurezza.

2. *Privacy by design*

Il Responsabile esterno garantisce che i principi di protezione dei dati e di sicurezza dei dati siano presi in considerazione durante i processi di progettazione e sviluppo dei sistemi IT. L'obiettivo è quello di prevenire un'attività di programmazione aggiuntiva, dispendiosa in termini di costi e di tempo, che sarebbe necessaria se i requisiti di *privacy* e sicurezza dei dati dovessero essere attuati dopo l'installazione dei sistemi IT. All'inizio del processo di sviluppo vengono prese in considerazione misure come la disattivazione di alcune funzionalità software, l'autenticazione, la pseudonimizzazione o la crittografia.

Il Responsabile esterno si assicura che siano trattati solo i dati personali necessari per il relativo scopo.

In particolare va assicurato il ricorso alla pseudonimizzazione dei dati in tutti i casi in cui non sia possibile o sostenibile cifrarli.

Inoltre i Responsabile esterno dovrà mettere in atto tutte le misure tecniche ed organizzative al fine di assicurare:

- la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;

- la verifica e la valutazione periodica dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Comunicazioni via e-mail

Considerato che il contenuto delle e-mail può essere visualizzato anche da terzi, le comunicazioni relative ad informazioni riservate non devono essere effettuate per e-mail non crittografate, quando la riservatezza delle informazioni trasmesse non può essere garantita.

4. Amministrazione da remoto

Nel caso i dipendenti o subappaltatori del Responsabile esterno debbano accedere ai dati dei soggetti interessati o del Titolare, l'accesso è disciplinato dalle seguenti regole generali:

- l’accesso all’amministrazione da remoto è chiuso per impostazione predefinita e viene autorizzato solo dall’Amministratore, il quale avrà la possibilità di monitorare gli interventi;
- le password per accedere ai sistemi IT vengono rilasciate dall’Amministratore solo per le finalità di cui all’Allegato A;
- gli interventi critici sono garantiti da una procedura “*4-eyes*” (principio del doppio controllo);
- l’accesso all’amministrazione da remoto viene registrato nel sistema. Vengono registrati i seguenti dati: persona responsabile, data e ora, durata, sistema di destinazione, breve descrizione dell’attività svolta e, in caso di interventi critici, i nominativi del personale qualificato aggiuntivo consultato nell’applicazione della procedura “*4-eyes*”;
- la registrazione delle sessioni di amministrazione da remoto è vietata, salvo i casi in cui sia necessaria per la risoluzione dei problemi segnalati dal Titolare.

5. Misure di sicurezza IT

Il Responsabile esterno rispetta delle “Misure minime di sicurezza ICT per le Pubbliche Amministrazioni”, emanate dall’AgID con circolare n. 2/2017 del 18 aprile 2017 in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015, si adegua a quanto prescritto dal Provvedimento del Garante della privacy del 27/11/2008 ed in particolare cura:

- la valutazione delle caratteristiche soggettive nell'attribuzione della funzione di amministratore di sistema o di applicativo;
- la designazione individuale dell'Amministratore di sistema o di applicativo con elencazione analitica degli ambiti di operabilità;
- l'elenco degli Amministratori di sistema o di applicativo;
- la conservazione gli estremi delle persone preposte quali Amministratori di sistema o di applicativo;
- la verifica delle attività degli amministratori di sistema o di applicativo almeno con cadenza annuale;
- la registrazione degli accessi logici agli archivi elettronici in elenchi aventi le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore ai 6 mesi.

6. Sicurezza perimetrale

Le reti informatiche del Responsabile esterno devono essere protette da sistemi di sicurezza perimetrale (c.d. *Firewall*) e da altre apparecchiature all’uopo destinate mantenute aggiornate allo stato dell’arte.

7. Protezione Antivirus

Ogni postazione di lavoro del Responsabile esterno deve essere protetta da sistemi di sicurezza contro le minacce informatiche (antivirus) e ne viene consentito l’utilizzo unicamente mediante appositi sistemi di autenticazione e di profilazione.

8. Altre misure

- Adottare opportune politiche di *data recovery* e *business continuity;*
- Garantire che le connessioni siano effettuate esclusivamente tramite protocollo HTTPS;
- Incrementare la consapevolezza dei soggetti autorizzati attraverso una serie di misure che implicano formazione, aggiornamento e accesso a procedure e *policy* specifiche in ambito *privacy* e

sicurezza, prevedendo contemporaneamente l'attribuzione di responsabilità specifiche e possibili provvedimenti in caso di mancato rispetto delle stesse o delle *policy;*

- Adottare opportune politiche per la gestione di eventuali casi di *data breach;*
- Attuare una gestione degli account utenti che consideri il ciclo di vita dell'account, dalla creazione alla dismissione dello stesso, prevedendo anche una procedura di revisione periodica;
- Gestire i log di accesso e gli eventuali accessi non autorizzati, impostando delle procedure specifiche per entrambe le situazioni, fornendo una debita informativa al Titolare e, nel caso, all'Autorità Garante