

REPUBBLICA ITALIANA  
REGIONE SICILIANA

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

**Responsabile esterno del trattamento dei dati personali relativi alle attività per l'espletamento delle procedure concorsuali previste dal Piano Triennale dei Fabbisogni del Personale 2020/2022**

**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";
- 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;
- 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. 2804 del 19 giugno 2019, con il quale alla dott. 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 regionale Marco Zambuto, nella qualità di Titolare del trattamento, conferma quanto disposto con D.A. n. 2896 del 25 giugno 2020, con il quale l'Assessore regionale pro tempore On.le Bernardette Grasso ha 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;

**Vista** la delibera della Giunta regionale n. 503 del 25 novembre 2021 con la quale, in conformità alla proposta nota prot. n. 125573 del 25 novembre 2021 dell'Assessore regionale per le Autonomie locali e per la Funzione pubblica e dell'Assessore regionale per il Territorio e l'Ambiente, è stato deliberato di individuare nel Dipartimento regionale della Funzione pubblica e del Personale il centro di responsabilità incaricato della definizione delle convenzioni con il Formez PA, finalizzate all'espletamento delle procedure concorsuali autorizzate dal Piano triennale dei fabbisogni del personale per il triennio 2020-2022 e relative integrazioni e adeguamenti, incluse quelle relative al Comando del corpo forestale della Regione Siciliana;

**Vista** la nota prot n. 127289 del 1/12/2021 avente per oggetto “Richiesta collaborazione per l'espletamento delle procedure concorsuali” con la quale il Dipartimento regionale della Funzione Pubblica e del Personale – Servizio 5° “Reclutamento, trasferimento e mobilità” ha richiesto al Formez PA con sede in viale Marx, 15 - 00137 Roma l'assistenza per l'organizzazione delle procedure concorsuali previste dal Piano Triennale dei Fabbisogni del Personale 2020/2022 e successive integrazioni e adeguamenti;

**Vista** la Convenzione stipulata tra la Regione Siciliana e Formez PA in data 20/12/2021 (nel seguito “Convenzione”) relativa all'organizzazione e alla realizzazione delle attività direttamente connesse alle procedure concorsuali per la selezione di n. 1.124 unità di personale di cui all'Allegato A della Convenzione con riferimento alla delibera della Giunta regionale n. 503 del 25 novembre 2021;

**Visto** il Decreto n. 4941 del 20/12/2021 a firma del Dirigente generale del Dipartimento regionale della Funzione pubblica e del Personale con il quale è stata approvata la Convenzione;

**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 e fornendogli le istruzioni necessarie;

**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 le specifiche istruzioni, ai sensi dell'art. 28 del Regolamento Ue 2016/679 del 27 aprile 2016, da fornire al Formez PA, quale Responsabile esterno del trattamento dei dati personali per l'attività di assistenza per l'organizzazione delle procedure concorsuali previste dal Piano Triennale dei Fabbisogni del Personale 2020/2022 e successive integrazioni e adeguamenti;

## DECRETA

### Art. 1 – Responsabile Esterno

1. Ai sensi dell'art. 28 del Regolamento Ue 2016/679 del 27 aprile 2016, Formez PA con sede in viale Marx, 15 - 00137 Roma (Formez PA) è stata nominata con nota prot. 129074 n. del 3/12/2021, quale Responsabile esterno del trattamento dei dati personali relativamente alle attività per l'espletamento delle procedure concorsuali in essa dettagliate, per le quali in data 20/12/2021 è stata stipulata la Convenzione tra l'Amministrazione regionale e Formez PA approvata con D.D.G. n. 4941 del 20/12/2021.
2. Il Responsabile esterno ha facoltà di designare sub-Responsabili del trattamento le società o i soggetti subappaltanti, previa comunicazione scritta da parte del Responsabile esterno e salvo diverso avviso della Regione Siciliana - 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 ad un mese dal completamento delle operazioni affidate 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.
4. L'Amministrazione prende atto del fatto che la Formez PA si avvale di CO.M.MEDIA S.r.l. con sede in via di Pettorano n. 22, Lecce per la gestione e l'implementazione del sistema informativo Step One e del Consorzio Digicontest con sede legale in largo Spinelli n. 12, Roma per il servizio integrato per l'organizzazione di concorsi pubblici e che pertanto gli stessi, nell'ambito del trattamento di dati personali di cui al presente decreto, operano quali sub-Responsabili sotto la diretta responsabilità di Formez PA ed ai quali quest'ultimo impone gli stessi obblighi in materia di protezione dei dati contenuti nel presente decreto, incluse le garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti richiesti dalle leggi applicabili e il contenuto del presente decreto.

## **Art. 2- Obblighi**

1. Il Responsabile esterno ha facoltà, nell'ambito dell'esecuzione del servizio affidato, di procedere alla nomina degli autorizzati al trattamento dei dati personali, mediante apposito atto di designazione. Per autorizzato si intende qualsiasi unità di personale individuata dal Responsabile esterno, che sia autorizzata al trattamento dei dati personali, secondo le direttive e istruzioni impartite dallo stesso Responsabile esterno. Il Responsabile esterno fornisce all'Amministrazione l'elenco degli autorizzati.
2. Il Responsabile esterno, nell'ambito dell'esecuzione del servizio affidato, 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 a quanto concordato con la Convenzione di cui all'art. 1.
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 ciascun 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;

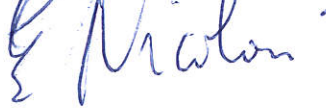
- j. fornire assistenza al Titolare per la valutazione d'impatto dell'eventuale uso di nuove tecnologie sulla sicurezza dei dati personali trattati (*data protection impact assessment* o DPIA o VIP);
  - k. comunicare al Titolare i dati di contatto del proprio "Responsabile della protezione dei dati", 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 norme, delle istruzioni di cui all'Allegato B al presente provvedimento o di quelle successive eventualmente trasmesse per iscritto dall'Amministrazione.
5. Il Responsabile esterno, ad un mese dal completamento del servizio affidato 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, 21 DIC 2021

Il Dirigente del Servizio  
Emanuele Nicolosi



Il Dirigente Generale  
C. Madonia



Allegato A

N	Denominazione del trattamento	Finalità del trattamento	Categorie di interessati	Categoria dati personali	Durata del trattamento	Responsabile esterno del trattamento
1	Attività per l'espletamento delle procedure concorsuali di cui alla Convenzione del 20/12/2021 tra l'Amministrazione regionale e Formez PA	Svolgimento delle procedure concorsuali di cui alla Convenzione del 20/12/2021 tra l'Amministrazione regionale e Formez PA	Candidati ammessi a partecipare alle procedure concorsuali di cui alla Convenzione del 20/12/2021 tra l'Amministrazione regionale e Formez PA	<ul style="list-style-type: none"> <li>• Dati personali di identificazione dei candidati e relativi recapiti anche informatici;</li> <li>• Dati relativi alle domande di partecipazione alle procedure concorsuali in argomento;</li> <li>• Eventuali condizioni di inabilità al fine di fornire i servizi di assistenza ai candidati portatori di handicap;</li> <li>• Punteggi conseguiti dai candidati nelle varie prove;</li> <li>• Dati inerenti la valutazione dei titoli (studio, servizio, preferenze e riserve) ai fini della stesura della graduatoria finale dei vincitori;</li> </ul>	Fino ad un mese dal completamento del servizio affidato o, comunque, in caso di cessazione – per qualunque causa – dell'efficacia del presente atto di nomina	Formez PA

## MISURE DI SICUREZZA

Per garantire la sicurezza dei dati, il Responsabile esterno adotta e rivede regolarmente le misure organizzative, tecniche, procedurali e logistiche sulla sicurezza dei trattamenti con riferimento all'art. 32 del Regolamento Ue 2016/679 e, tenendo conto dello stato dell'arte delle tecnologie di sicurezza e della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio per i diritti e le libertà delle persone fisiche, si assicura che le misure di sicurezza adottate siano adeguate a garantire un livello di sicurezza adeguato al rischio, in particolare contro la distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trattati e il trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento.

Ciò include la determinazione di scenari di danno tipici, delle esigenze di sicurezza e dei livelli di sicurezza che sono associati ai diversi tipi di dati personali, l'esecuzione di valutazioni di impatto sulle libertà personali e sui diritti dell'interessato, la nomina formale di uno o più Amministratore di sistema, l'adozione di politiche di gestione e di accesso ai dati personali.

In merito agli autorizzati al trattamento, il Responsabile esterno assicura il Titolare che abbiano ricevuto adeguata formazione in materia di protezione dei dati e cura la vigilanza sul loro operato, vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento delle loro attività, anche successivamente alla cessazione del rapporto di lavoro/collaborazione con il Responsabile del trattamento.

Inoltre, il Responsabile esterno predisporre ed attua:

- verifiche di vulnerabilità dei sistemi, finalizzate ad analizzare, esaminare e valutare regolarmente che la sicurezza dei sistemi sia adeguata alle misure tecniche e organizzative adottate;
- opportune politiche di *data recovery* e *business continuity*;
- opportune politiche per l'incremento della consapevolezza, affidabilità e competenza dei soggetti autorizzati attraverso la formazione, l'aggiornamento e l'accesso a procedure e modelli comportamentali specifici in ambito *privacy* e sicurezza, prevedendo contemporaneamente l'attribuzione di responsabilità specifiche e possibili provvedimenti in caso di mancato rispetto delle stesse;
- opportune politiche conformi alle disposizioni del Titolare per la gestione di eventuali casi di *data breach* con particolare riferimento alle "Procedura di risposta ad una violazione dei dati personali" approvata con Delibera di giunta regionale n. 483 del 29/11/2019.

I seguenti aspetti concorrono a disciplinare l'attuazione di misure tecniche e organizzative appropriate.

### **1. Backup dei dati**

Per evitare distruzione o perdita di dati, il Responsabile esterno definisce ed attua direttamente o con il supporto di altri sub-Responsabili appositamente individuati, idonee procedure affinché i dati vengono regolarmente sottoposti a *backup* sulla base di apposite procedure di sicurezza IT e per la verifica dell'efficacia delle copie di sicurezza. Inoltre custodisce le stesse con modalità adeguate contro la divulgazione non autorizzata o l'accesso accidentale o illegale.

### **2. Privacy by design e by default**

Il Responsabile esterno garantisce che i principi di protezione dei dati e di sicurezza dei dati siano presi in considerazione in fase di progettazione e sviluppo dei sistemi IT, garantendo una adeguata sicurezza per impostazione predefinita mediante misure quali ad es. la disattivazione di alcune funzionalità software, l'autenticazione e la registrazione degli accessi, la pseudonimizzazione dei dati o la crittografia.



Il Responsabile esterno si assicura preliminarmente che siano trattati solo i dati personali necessari per il relativo scopo e ricorre alla pseudonimizzazione dei dati in tutti i casi in cui non sia possibile o non sia sostenibile cifrarli.

Inoltre il Responsabile esterno predispone adeguate misure 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 del corretto funzionamento dei sistemi e degli applicativi e dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

### **3. Comunicazioni dei dati personali**

Fermo restando che la comunicazione dei dati personali viene effettuata solo nei confronti di soggetti aventi titolo ai sensi delle norme vigenti e in particolare del Regolamento Ue 2016/679, quando vengono trasmesse informazioni personali la cui divulgazione ha rilievo in termini di limitazione dei diritti e delle libertà personali degli interessati, il Responsabile esterno adotta apposite misure di protezione o di criptazione, atte a garantire la sicurezza contro la divulgazione, anche accidentale, delle stesse.

Qualora il Responsabile esterno ritenga che per la realizzazione delle attività ad esso affidate sia necessario il trasferimento dei dati personali in argomento in sistemi ubicati al di fuori dall'Unione europea, si accerta e ne dà assicurazione al Titolare, che il suddetto trasferimento e la permanenza dei dati in tali sistemi avviene con rispetto delle norme in tema di protezione dei dati personali ed in particolare del Regolamento Ue 2016/679.

### **4. 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 dai provvedimenti del Garante della protezione dei dati personali ed in particolare cura:

- la valutazione delle caratteristiche soggettive nell'attribuzione della funzione di Amministratore di sistema o di applicativo;
- la designazione formale di uno o più Amministratore di sistema o di applicativo con elencazione analitica degli ambiti di operabilità;
- l'elencazione degli Amministratori di sistema o di applicativo e la conservazione dei rispettivi recapiti;
- la verifica delle attività degli Amministratori di sistema o di applicativo almeno con cadenza annuale;
- che gli interventi critici e quelli riguardanti la sicurezza siano attuati da una procedura che rispetta il principio del doppio controllo, nel quale vengono coinvolti un minimo di due persone, ovvero il promotore dell'intervento e il responsabile della verifica. Le informazioni relative all'intervento messo in atto e gli estremi dei soggetti intervenuti vanno memorizzate in un apposito log, assieme alle informazioni temporali e ai sistemi su cui è stato effettuato l'intervento;
- che le reti informatiche gestite siano protette da sistemi di sicurezza perimetrale (c.d. *Firewall*) e da altre apparecchiature all'uopo destinate mantenute aggiornate allo stato dell'arte;
- che le postazioni di lavoro utilizzate siano mantenute aggiornate e protette da sistemi di sicurezza contro le minacce informatiche (ad es. antivirus) e ad esse si possa accedere unicamente mediante appositi sistemi di autenticazione e di profilazione;

- che la gestione degli account utenti consideri il ciclo di vita dell'account, dalla creazione alla dismissione dello stesso, prevedendo anche una procedura di revisione periodica;
- che le connessioni ai server web utilizzati e gestiti siano effettuate esclusivamente tramite protocollo https.

#### **4. Accesso da remoto ai sistemi IT**

Nel caso i soggetti autorizzati al trattamento dal Responsabile esterno o i sub-Responsabili dallo stesso designati debbano accedere ai dati dei soggetti interessati o del Titolare depositati in sistemi IT di competenza del Responsabile esterno, l'accesso è disciplinato dalle seguenti regole generali:

- le password e le autorizzazioni per accedere ai sistemi IT vengono rilasciate dall'Amministratore di sistema solo per le finalità di cui all'Allegato A;
- di ogni accesso logico agli archivi elettronici vengono registrati i riferimenti temporali (inizio e fine), il nome dell'account, sistema o applicativo su cui opera e la descrizione dell'attività svolta secondo le indicazioni stabilite dall'Amministratore. Tali informazioni vengono memorizzate 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 essere conservate per un congruo periodo, non inferiore ai 6 mesi;
- l'accesso da remoto per attività di amministrazione dei sistemi IT e degli applicativi è chiuso per impostazione predefinita e viene autorizzato laddove necessario dall'Amministratore di sistema, il quale avrà la possibilità di monitorare gli interventi e di accedere alle relative registrazioni, senza possibilità di modifica o cancellazione da remoto.