



*Regione Siciliana*  
*Assessorato dell'Economia*  
*Autorità Regionale per l'Innovazione Tecnologica*

**IL DIRIGENTE GENERALE**

- VISTO lo Statuto della Regione siciliana;
- VISTA la legge regionale 29 dicembre 1962, n.28;
- VISTA la legge regionale 10 aprile 1978, n.2;
- VISTO il D.P.R.S. n.12 del 14 giugno 2016 concernente “Regolamento di attuazione del Titolo II della L.R. 7 maggio 2015, n.9 “Modifica del decreto del Presidente della Regione 18 gennaio 2013, n. 6” e s.m.i.;
- VISTO il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016 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”;
- VISTA la deliberazione della Giunta regionale n. 203 del 28/05/2018 in tema di “Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 - Nomina del Responsabile per la protezione dei dati”;
- VISTO il Regolamento UE/2016/679 ed in particolare l'art. 27 recante “Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione”;
- VISTO il Regolamento UE/2016/679 ed in particolare l'art. 28, commi 2 e 4, recante “Responsabile del Trattamento”;
- VISTO il D.P.R.S. 12 giugno 2018, n. 569 con il quale l'Ing. Sebastiano Lio, dirigente di 3^ fascia dell'Amministrazione Regionale, è stato nominato “Responsabile della protezione dei dati” per la Regione siciliana;
- VISTO il D.lgs del 10 agosto 2018, n. 101 recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati)” pubblicato nella G.U. n. 205 del 04/09/2018.
- VISTA la deliberazione della Giunta Regionale di Governo 29 novembre 2018 n. 483, recante “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.Reg. n.777/Area 1/SG del 15/11/2022 con il quale l'on.le Marco Falcone è stato nominato Assessore regionale dell'Economia;
- VISTA la nota prot. n. 7564/Gab del 17/11/2022 concernente l'insediamento dell'On.le Marco Falcone in qualità di Assessore regionale dell'Economia;

- VISTO il D.P. n. 432 del 13.02.2023 con il quale, in esecuzione della deliberazione della Giunta Regionale n. 79 del 10.02.2023, alla dott.ssa Vitalba Vaccaro, dirigente di 3<sup>a</sup> fascia dell'Amministrazione regionale, è stato conferito l'incarico di Dirigente Generale dell'Ufficio di Coordinamento dei Sistemi Informativi Regionali e l'Attività Informatica della Regione e delle Pubbliche Amministrazioni Regionali, in atto denominato Autorità regionale per l'Innovazione Tecnologica dell'Assessorato Regionale dell'Economia, per la durata di anni due con decorrenza dal 14.02.2023, data in cui ha assunto le relative funzioni;
- VISTO il D.A. n.15/GAB del 30.03.2023 con il quale l'Assessore dell'Economia ha approvato il contratto individuale di lavoro del Dirigente Generale dell'Autorità Regionale per l'Innovazione Tecnologica dell'Assessorato Regionale dell'Economia, stipulato in data 30.03.2023 tra l'Assessore Regionale dell'Economia e la Dott.ssa Vitalba Vaccaro;
- VISTO in particolare l'articolo 10 del contratto individuale di lavoro con il quale, ai sensi del comma 4 dell'art.28 del Regolamento UE 2016/679, in applicazione della Delibera di Giunta Regionale n.483 del 29.11.2018, la Dott.ssa Vitalba Vaccaro assume le funzioni di Responsabile dei Trattamenti di dati personali attinenti le materie trattate dall'Autorità Regionale per l'Innovazione Tecnologica;
- VISTO il D.D.G. n. 380 del 28 dicembre 2022 con cui è stato approvato il contratto di servizio stipulato tra l'Autorità Regionale per l'Innovazione Tecnologica (ARIT) e la Società in-house Sicilia Digitale S.p.A. per le attività informatiche dell'Amministrazione regionale;
- VISTO in particolare, l'Art. 13 (Obbligo di riservatezza) del Contratto di servizio con il quale al comma 2 viene individuata la società Sicilia Digitale S.p.A. quale Responsabile esterno del trattamento dei dati, nel rispetto di quanto previsto dal Regolamento Europeo n. 679/2016 (c.d. "GDPR"), e che con la sottoscrizione del contratto di servizio la citata Società si impegna ed accetta la designazione a Responsabile/sub-Responsabile esterno del trattamento ai sensi dell'art. 28 del Regolamento UE da parte dell'Amministrazione Regionale relativamente ai dati personali di cui la stessa è Titolare e che potranno essere trattati dalla Società contraente nell'ambito dell'erogazione dei servizi previsti in contratto;
- CONSIDERATO quindi, che ai fini del D.Lgs. 30 giugno 2003, n. 196, e s.m.i., rispetto alla tutela dei dati personali, la società Sicilia Digitale S.p.A. è responsabile del trattamento dei dati personali di cui viene in possesso nell'espletamento dei servizi affidati, avendo cura di utilizzarli conformemente alle previsioni normative ed esclusivamente per gli adempimenti finalizzati agli obblighi di cui al citato contratto di servizio, e che qualora il fornitore sia chiamato ad eseguire le 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 Parlamento Europeo e del Consiglio del 27-4-2016, attribuendogli le relative competenze;
- CONSIDERATO che Sicilia Digitale S.p.A., nella qualità di Responsabile esterno del trattamento dei dati, si obbliga ad adottare le misure di sicurezza di natura fisica, logica, tecnica ed organizzativa idonee a garantire un livello di sicurezza adeguato ai rischi e conformi alla normativa vigente ed alle istruzioni fornite dall'Amministrazione Regionale;

RITENUTO per le motivazioni indicate in premessa, di dover nominare ai sensi dell'art. 28 del Regolamento UE 2016/679, Responsabile esterno del trattamento dei dati personali relativi al Contratto di servizio delle attività informatiche la società Sicilia Digitale S.p.A.;

## **DECRETA**

### **Art. 1 – Nomina**

1. Ai sensi dell'art. 28 del Regolamento UE 2016/679, nell'ambito e per conto dell'Assessorato Regionale per l'Economia, quale titolare del trattamento dei dati, e dell'A.R.I.T. nella qualità di Responsabile del trattamento dei dati, il Dirigente Generale dell'A.R.I.T. designa la Società Sicilia Digitale S.p.A. quale Responsabile esterno del Trattamento dei dati per l'esecuzione del contratto di servizio delle attività informatiche stipulato in data 28/12/2022 ed approvato con D.D.G. n. 380/2022 nel rispetto dell'art. 13 del contratto di servizio stesso.
2. Il Responsabile esterno del trattamento ha facoltà di designare sub-Responsabili del trattamento le società subappaltanti, previa autorizzazione scritta da parte del Titolare del Trattamento dei dati.
3. Il Responsabile esterno effettua il trattamento dei dati di tutti i servizi informatici oggetto del contratto di servizio e relativi ai sistemi informativi meglio specificati nell'Allegato H facente parte integrante del contratto. Nel rispetto di quanto stabilito nel citato D.A. n. 15/GAB e nel contratto individuale di lavoro con lo stesso approvato, nell'Allegato A del presente decreto viene individuato il registro delle attività di trattamento dei dati personali trattati per conto del Titolare.
4. La nomina di Responsabile esterno del trattamento dei dati ha validità dalla operatività del Contratto di cui al comma 1 del presente articolo è valida fino alla vigenza del contratto stesso, o fino alla revoca anticipata per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione del Contratto di fornitura 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 del trattamento, nell'ambito dell'esecuzione dei contratti di cui all'art.1, provvederà nel rispetto del comma 4 dell'Art. 13 del contratto di servizio alla nomina dei soggetti delegati al trattamento dei dati personali, mediante apposito atto di designazione. Per autorizzato si intende qualsiasi unità di personale interna alla propria società, autorizzata al trattamento dei dati personali secondo le proprie direttive e istruzioni. Il Responsabile esterno fornisce, all'Autorità Regionale per l'Innovazione Tecnologica l'elenco degli autorizzati.
2. Il Responsabile esterno del trattamento, nell'ambito dell'esecuzione dei contratti di cui all'art. 1, 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 si deve attenere alle misure di sicurezza indicate dall'ARIT, di cui all'Allegato B al presente provvedimento, nonché di quelle specificate nel contratto di servizio di cui all'art. 1 e relativi allegati.
4. Il Responsabile esterno del trattamento 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 atto e vigila sul loro rispetto. Il Responsabile esterno del trattamento rimarrà direttamente responsabile nei confronti del Titolare in ordine alle azioni ed alle omissioni dei propri sub-Responsabili.

### **Art. 3 – Oneri e Responsabilità**

1. Il Responsabile esterno del trattamento 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 del trattamento 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 Europeo UE 2016/679;
  - 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 deputati 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 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 l'ARIT nell'aggiornamento dei registri delle categorie di attività di trattamento;
  - e. cooperare, su richiesta, assieme al Titolare, con l'Autorità di controllo 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. 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;
  - l. 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 UE;
  - m. Fornire assistenza al titolare nell'aggiornamento della informativa da rendere agli interessati ai sensi degli art. 13 e 14 del Regolamento UE 679/2016 in merito al trattamento in argomento;
  - n. Rendere disponibili tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dal Regolamento Europeo UE 2016/679.



3. Il Responsabile esterno del trattamento 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 ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR. Inoltre comunica le prime misure organizzative e tecniche adottate per porre rimedio alla violazione dei dati personali e per minimizzare gli effetti negativi e propone al Titolare l'adozione di ulteriori misure di sicurezza non immediatamente attuabili.
4. Il Responsabile esterno del trattamento 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'Assessorato Regionale dell'Economia.
5. Il Responsabile esterno del trattamento, all'atto della scadenza del Contratto di Servizio 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. 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.

Il presente D.D.G. è trasmesso al responsabile del procedimento di pubblicazione dei contenuti sul sito istituzionale, ai fini dell'art. 68 della l.r. n. 21/2014 per la registrazione di competenza.

Palermo, lì 19/12/2023

Il Dirigente Generale  
(*Vitalba Vaccaro*)

## Allegato A

Titolare		Assessore all'Economia				
Denominazione del trattamento	Finalità del trattamento	Categorie di interessati	Categoria dati personali	Durata del trattamento	Responsabili esterni del trattamento	Nella qualità di
Gestione presenze del personale ARIT	Gestione del personale	Dipendenti	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
Gestione protocollo informatico e corrispondenza	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
Rimborso spese per missioni	Gestione del personale	Dipendenti	dati personali di identificazione	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
Affidamento mediante contratto di fornitura di beni e servizi non informatici	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
Rilascio kit digitale e certificazione relativa	Gestione del personale e Amministratori	Dipendenti e Amministratori	dati personali di identificazione	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
affidamento mediante contratto di servizi della gestione di infrastrutture informatiche	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
affidamento mediante contratto di servizi della gestione di servizi informatici	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
affidamento mediante contratto di servizi della gestione di basi-dati	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
affidamento mediante incarico specifico della gestione d'infrastrutture informatiche	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
affidamento mediante incarico specifico della gestione di servizi informatici	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
affidamento mediante incarico specifico della gestione di basi dati	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche
affidamento mediante incarico specifico della gestione di basi dati e applicativi in ambito sanitario	Gestione del personale e utenti esterni	Dipendenti e utenti esterni	dati personali di identificazione, dati sulla salute fisica, inclusi dati sanitari e dati giudiziari	fino al 31/12/2024 salvo proroghe e/o sospensioni	Sicilia Digitale s.p.a.	Società affidataria del servizio di assistenza delle attività informatiche

## Allegato B

### **MISURE DI SICUREZZA**

Per garantire la sicurezza dei dati, il Responsabile esterno del trattamento rivede regolarmente lo stato dell'arte delle tecnologie di sicurezza. 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, nonché l'esecuzione di valutazioni del rischio. Inoltre, vengono effettuati test di penetrazione dedicati per analizzare, esaminare e valutare regolarmente l'efficacia di queste misure tecniche e organizzative che devono garantire la sicurezza del trattamento.

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

#### **Backup dei dati**

Per evitare perdite, il Responsabile esterno del trattamento 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.

#### **“Privacy by design”**

Il Responsabile esterno del Trattamento garantisce che i principi di protezione/privacy 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 o la crittografia.

Devono essere 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 il 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

#### **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 poiché la riservatezza delle informazioni trasmesse non può essere garantita.

#### **Amministrazione da remoto**

Nel caso i dipendenti o subappaltatori del Responsabile esterno del trattamento debbano accedere ai dati dei soggetti istanti 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) con ulteriore presenza dell'interessato;
- l'accesso all'amministrazione da remoto viene registrato nel sistema CRM. 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.

### **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 e nella qualità di Amministratore di sistema si adegua a quanto prescritto dal Provvedimento del Garante della privacy del 27/11/2008 ed in particolare cura:

1. la valutazione delle caratteristiche soggettive nell'attribuzione della funzione di amministratore di sistema;
2. la designazione individuale dell'amministratore di sistema con elencazione analitica degli ambiti di operabilità;
3. l'elenco degli amministratori di sistema
4. la conservazione gli estremi delle persone preposte quali amministratori di sistema;
5. la verifica delle attività degli amministratori di sistema almeno con cadenza annuale;
6. 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.

#### **1. Firewall o sicurezza perimetrale**

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

#### **2. Protezione Antivirus**



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

### **Altre Misure**

- Adottare opportune politiche di *disaster 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 security, 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.