D.R.S. n. 90 del 21.05.2025

REPUBBLICA ITALIANA

REGIONE SICILIANA

Istruzioni per il trattamento dei dati personali relativi alla piattaforma informatica per il canale interno di segnalazione di condotte illecite "W*histleblowing"*

Visto lo Statuto della Regione Siciliana;

Vista 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 27-4-2016 – 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*";

Vista la deliberazione della Giunta Regionale di Governo 8 agosto 2019 n. 297, *"Regolamento UE 2016/679 – Organizzazione dell'Amministrazione regionale per gli adempimenti in materia di privacy"* concernente la delega ai Responsabili del trattamento da parte del Presidente e degli Assessori regionali dei poteri che riguardano adempimenti operativi, quali la nomina dei sub-Responsabili;

Visto il D.P.Reg. 20 maggio 2025, n. 540/Gab con il quale è stato designato il Responsabile della protezione dei dati per la Regione Siciliana;

Visto il D.D.G. n. 11 del 21 gennaio 2025 con cui è stato approvato il contratto di servizio stipulato tra l'Autorità regionale per l'Innovazione Tecnologica (ARIT) e la società Isweb s.p.a. per l'acquisizione del sistema interno di segnalazioni *whistleblowing* in modalità cloud *Software As A Service* (SAAS) per la Regione siciliana;

Visto il Contratto n. 8293109 del 20.01.2025 stipulato tra l'Autorità regionale per l'Innovazione Tecnologica (ARIT) e la società Isweb s.p.a. per l'acquisizione del sistema

interno di segnalazioni *whistleblowing* in modalità cloud *Software As A Service* (SAAS) per la Regione siciliana;

Visto il d.lgs. 10 marzo 2023, n. 24 "*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali";*

Visto l'art. 4, comma 1, del d.lgs. n. 24/2023 intitolato " *Canali di segnalazione interna*" ai sensi del quale "*i soggetti del settore pubblico e i soggetti del settore privato, sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivano, ai sensi del presente articolo, propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. I modelli di organizzazione e di gestione, di cui all'articolo 6, comma 1, lettera a), del decreto legislativo n. 231 del 2001, prevedono i canali di segnalazione interna di cui al presente decreto*";

Visto l'art. 4, comma 4, del citato d.lgs. n. 24/2023, secondo cui, "*I soggetti del settore pubblico cui sia fatto obbligo di prevedere la figura del responsabile della prevenzione della corruzione e della trasparenza, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, affidano a quest'ultimo, anche nelle ipotesi di condivisione di cui al comma 4, la gestione del canale di segnalazione interna";*

Visto il D.P. n. 557 del 17 luglio 2023, con cui il Responsabile per la Prevenzione della Corruzione e per la Trasparenza avv. Emanuela Giuliano è stata designata quale Responsabile del trattamento dei dati per il sistema di segnalazione di condotte illecite di *whistleblowing*, ai sensi dell'art. 28 del Regolamento UE 2016/679, nell'ambito e per conto della Presidenza della Regione quale Titolare del trattamento;

Considerato che qualora un soggetto 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 quindi, di dovere individuare, ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016, la società Isweb s.p.a. con sede in via Luigi Cadorna, 31 – 67051 Avezzano (AQ) - P.IVA 01722270665, quale Responsabile esterno del trattamento dei dati personali relativamente al sistema interno di segnalazioni *whistleblowing* in modalità cloud *Software As A Service* (SAAS) per la Regione siciliana, di cui al DDG. n. 11 del 21 gennaio 2025 con cui è stato approvato il contratto di servizio n. 8293109 del 20.01.2025 stipulato tra l'Autorità regionale per l'Innovazione Tecnologica (ARIT) e la società Isweb s.p.a.;

DECRETA

Art. 1 – Responsabile esterno

1. Ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016 (nel seguito "GDPR"), il Responsabile del trattamento dei dati individua la società Isweb s.p.a con sede in via Luigi Cadorna, 31 – 67051 Avezzano (AQ) - P.IVA 01722270665, quale Responsabile esterno del trattamento dei dati personali relativamente al sistema interno di segnalazioni *whistleblowing* in modalità cloud *Software As A Service* (SAAS) per la Regione siciliana, di cui al DDG. n. 11 del 21 gennaio 2025 con cui è stato approvato il contratto di servizio n. 8293109 del 20.01.2025 stipulato tra l'Autorità regionale per l'Innovazione Tecnologica (ARIT) e la società Isweb s.p.a..
2. Il Responsabile esterno ha facoltà di designare sub-Responsabili del trattamento le società o i soggetti subappaltanti, previa autorizzazione scritta da parte del Titolare del trattamento dei dati.
3. Il Responsabile esterno effettua il trattamento dei dati di cui all'allegato "A" del presente provvedimento nei limiti e nel rispetto delle finalità per cui sono stati raccolti. La nomina di Responsabile esterno ha validità dalla data di inizio operatività del Contratto ed è valida fino alla vigenza del Contratto stesso, o fino alla revoca anticipata per qualsiasi motivo da parte dell'Amministrazione, fermo restando che, anche successivamente alla cessazione del Contratto o alla revoca, il Responsabile esterno dovrà mantenere la massima riservatezza sui dati e le informazioni delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

Art. 2 - Obblighi

1. Il Responsabile esterno ha facoltà, nell'ambito dell'esecuzione del Contratto, 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, adeguatamente formata, sia stata autorizzata al trattamento dei dati personali secondo le direttive e le istruzioni impartite dalla Società stessa. Il Responsabile esterno fornisce all'Amministrazione l'elenco degli autorizzati.
2. Il Responsabile esterno, nell'ambito dell'esecuzione del Contratto, 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, inoltre, si atterrà alle misure di sicurezza indicate dall'Amministrazione, di cui all'Allegato "B" al presente decreto, nonché di quelle specificate nel Contratto, come rese note all'ARIT nel documento "Dichiarazione sulle Misure di Sicurezza – Allegato all'offerta – Rev. 03.05.2024 e da ogni ulteriore comunicazione in merito non in contrasto con le presenti istruzioni.
4. Il Responsabile esterno, autorizzato, per l'erogazione dei servizi di data-center, a ricorrere al sub-Responsabile Seeweb srl - Corso Lazio n. 9/A – 03100 Frosinone, ha l'onere di informare l'Amministrazione di eventuali modifiche riguardanti l'aggiunta o la sostituzione di ulteriori sub-Responsabili. La responsabilità del sub-responsabile ricade sul responsabile ai sensi di quanto previsto dall'art. 28, comma 4, del Regolamento UE 2016/679.

L'Amministrazione 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 l'Amministrazione 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 dell'Amministrazione 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 GDPR.

Art. 3 - Oneri e Responsabilità

1. Il Responsabile esterno esegue i trattamenti delegati secondo le istruzioni ricevute dall'Amministrazione e supporta, per quanto di propria competenza, la stessa Amministrazione nel fornire risposta alla richiesta di esercizio dei diritti degli interessati relativi ai trattamenti delegati.
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 dell'Amministrazione è effettuato in conformità al GDPR;
   b) adottare misure tecniche e organizzative idonee a garantire la sicurezza dei locali e delle postazioni di lavoro dei soggetti autorizzati a trattare i dati personali;
   c) fornire ai propri dipendenti e collaboratori autorizzati 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) non cedere, non consegnare, non copiare, non riprodurre, non comunicare, non divulgare, non rendere disponibili in qualsiasi modo o a qualsiasi titolo a terzi, le informazioni acquisite nell'ambito dalle attività contrattuali;
   e) predisporre ed aggiornare sistematicamente il proprio registro delle attività di trattamento dei dati personali trattati per conto dell'Amministrazione ed assistere quest'ultimo nell'aggiornamento del registro delle categorie di trattamento e del registro delle categorie di attività di trattamento;
   f) cooperare, su richiesta, dell'Amministrazione, con il Garante della protezione dei dati personali (nel seguito "Autorità Garante") nell'esecuzione dei suoi compiti;
   g) fornire, nei limiti di quanto concerne i trattamenti delegati, assistenza all'Amministrazione per la gestione del consenso degli interessati al trattamento dei dati personali;
   h) fornire assistenza all'Amministrazione per informare in maniera trasparente gli interessati sulla modalità di gestione e di protezione dei relativi dati personali trattati;
   i) fornire assistenza per la gestione delle richieste degli interessati sui propri dati personali trattati per conto dell'Amministrazione;
   j) fornire assistenza all'Amministrazione per l'analisi del rischio sui dati personali trattati;

k) fornire assistenza all'Amministrazione per la valutazione d'impatto sulla protezione dei dati personali ai sensi dell'art. 35 del GDPR (*data protection impact assessment* o DPIA), laddove l'Amministrazione ritenga che ne ricorrano i requisiti;

l) comunicare all'Amministrazione 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 GDPR; il Responsabile esterno collabora e si tiene in costante contatto con il Responsabile della protezione dei dati della Regione Siciliana, rispondendo prontamente alle sue richieste;

m) collaborare con l'Amministrazione 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 GDPR;

n) 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 all'Unione Europea;

o) fornire assistenza all'Amministrazione nell'aggiornamento della informativa da rendere agli interessati ai sensi degli artt. 13 e 14 del GDPR in merito al trattamento in argomento;

p) rendere disponibili tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dal GDPR;

q) informare immediatamente l'Amministrazione qualora, a suo parere, un'istruzione dallo stesso fornita violi il GDPR o altre norme applicabili in materia di protezione dei dati;

r) ove risulti che le misure adottate dal Responsabile esterno o da un sub-Responsabile non siano idonee ad assicurare l'applicazione del GDPR o che non siano correttamente applicate, adottare e fare 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 dall'Amministrazione. 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 informa l'Amministrazione (inviando una comunicazione a mezzo PEC), senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza, in merito a qualsiasi elemento che possa compromettere il corretto trattamento dei dati personali e ad 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 all'Amministrazione in relazione all'adempimento degli obblighi, sullo stesso gravanti, di notifica delle suddette violazioni all'Autorità Garante ai sensi dell'art. 33 del GDPR 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 all'Amministrazione l'adozione di ulteriori misure di sicurezza non immediatamente attuabili. Il Responsabile esterno fornisce all'Amministrazione tutto il necessario supporto e la collaborazione per il riscontro alle richieste di informazioni aggiuntive da parte dell'Autorità Garante.

4. Il Responsabile esterno manleva e tiene indenne l'Amministrazione da qualsiasi danno, pretesa, risarcimento e/o sanzione che possa derivare dalla mancata osservanza degli obblighi e più in generale dalla violazione della normativa sulla tutela dei dati personali, nonché per le conseguenze derivanti dagli inadempimenti o inosservanze delle istruzioni di cui all'Allegato B al presente provvedimento o di quelle successive eventualmente trasmesse per iscritto per conto dell'Amministrazione.
5. Il Responsabile esterno, alla scadenza del Contratto o, comunque, in caso di cessazione per qualunque causa dell'efficacia della nomina a Responsabile esterno, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario, sarà tenuto ad interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, a scelta dell'Amministrazione, 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 dell'Amministrazione, 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 ai sensi della l.r. 12 agosto 2014, n. 21 e s.m.i.

Palermo

IL DIRIGENTE DEL SERVIZIO 5 -RESPONSABILE
PER LA PREVENZIONE DELLA CORRUZIONE
E PER LA TRASPARENZA
Emanuela Giuliano

EMANUELA GIULIANO
REGIONE SICILIANA
DIRIGENTE
21.05.2025 15:45:49 GMT+02:00

Allegato A

Titolare del trattamento	*Presidenza della Regione*
Responsabile del trattamento	*Responsabile per la Prevenzione della Corruzione e per la Trasparenza*
Responsabile esterno	*Società Isweb*
Data Protection Officer Responsabile Esterno	*dpo@isweb.it – dpo@pec.isweb.it*

N.	Denominazione del trattamento	Finalità del trattamento	Categorie di interessati	Categoria dati personali	Durata del trattamento
1	Sistema interno di segnalazioni *whistleblowing* in modalità cloud *Software As A Service* (SAAS) "Tipologia di trattamento: nello specifico i trattamenti oggetto di delega sono quelli indicati nella documentazione contrattuale e in particolare: memorizzazione, raggiungibilità via internet (messa a disposizione), gestione dei log del web server e degli accessi degli amministratori del sistema, backup, verifica della funzionalità dei backup, ripristino dati, cancellazione"	Esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri	Utenti interni/esterni	dati personali di identificazione, di recapito, dati relativi alla mansione lavorativa	fino alla vigenza del contratto

MISURE DI SICUREZZA

Il Responsabile esterno rispetta le "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 alle "Linee guida per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio" dell'Agenzia per la Cybersicurezza Nazionale.

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 GDPR 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 aggiornate ai più recenti standard ed adeguate a garantire un livello di sicurezza commisurato 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 l'Amministrazione 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 esterno.

Il Responsabile esterno si impegna ad accedere esclusivamente ai sistemi e ai dati cui ha la necessità nell'ambito delle attività previste dal Contratto.

Inoltre, il Responsabile esterno predispone 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 la verifica della affidabilità e l'incremento della consapevolezza e della 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 dell'Amministrazione per la gestione di eventuali casi di *data breach* con particolare riferimento alle "Procedura di risposta ad una violazione dei dati personali" approvata con deliberazione della Giunta regionale n. 483 del 29.11.2019.

I seguenti aspetti disciplinano l'attuazione di misure tecniche e organizzative appropriate da parte del Responsabile esterno.

1. 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 esempio la disattivazione di alcune funzionalità software, l'autenticazione e la registrazione degli accessi, la pseudonimizzazione dei dati o la crittografia.

Inoltre il Responsabile esterno predispone adeguate misure al fine di assicurare nei sistemi utilizzati:

- 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.

2. Comunicazioni

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 GDPR, 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.

3. Misure di sicurezza IT sugli accessi logici ai dati

Il Responsabile esterno adotta apposite misure di sicurezza in merito agli accessi logici agli applicativi e ai dati memorizzati in sistemi IT 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;

- la verifica dell'affidabilità del personale, sia prima dell'incarico che durante l'effettivo esercizio dei privilegi, sia in relazione al personale interno che ad eventuali fornitori esterni con accesso privilegiato all'infrastruttura o ai dati dell'Amministrazione;

- 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 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 le password e le autorizzazioni per accedere ai sistemi IT vengano rilasciate dall'Amministratore di sistema solo per le finalità di cui all'Allegato A;

- che la gestione delle utenze 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;

- che le utenze del personale e le relative credenziali di accesso a sistemi e banche dati siano nominative e individuali, cioè, non condivise tra più persone, anche al fine di poter tracciare gli

accessi e poter risalire in modo inequivocabile al personale interno ed esterno che effettua gli accessi;

- che nel caso di "utenze di sistema", per loro natura impersonali in quanto utilizzati da applicativi software, siano garantita una gestione sicura, volta a mitigare sia il rischio di utilizzo diretto da parte del personale dell'Amministrazione, sia quello di impossessamento in generale;
- che a ciascuna utenza siano assegnati privilegi e autorizzazioni di accesso minimi, strettamente necessari a svolgere i compiti assegnati al relativo ruolo e che rispettino il principio di segregazione delle funzioni;
- che le utenze, i relativi privilegi e credenziali siano verificate, aggiornate, revocate e sottoposte a audit periodicamente, secondo una cadenza temporale coerente con l'analisi dei rischi, considerando la criticità dei sistemi e delle banche dati cui possono accedere e il tipo di operazioni che possono effettuare;
- che le utenze e le relative credenziali siano aggiornate tempestivamente, e senza ingiustificato ritardo, in seguito a variazioni delle utenze (es. trasferimento di personale) e, in particolare, siano revocate tempestivamente per il personale cessato;
- che di ogni accesso logico agli archivi elettronici vengano 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 saranno 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 saranno conservate per un congruo periodo, non inferiore ai 6 mesi;
- che l'accesso da remoto per attività di amministrazione dei sistemi IT e degli applicativi sia chiuso per impostazione predefinita e che venga 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.

4. Accesso fisico ai sistemi IT

Nel caso i soggetti autorizzati al trattamento dal Responsabile esterno o i sub-Responsabili dallo stesso designati debbano accedere a sistemi di elaborazione e memorizzazione relativi ai dati dei soggetti interessati o dell'Amministrazione, nonché i sistemi per l'interconnessione su rete su cui insistono i sistemi stessi, l'accesso è disciplinato dalle seguenti regole generali:

- in virtù della possibilità di accesso ai sistemi IT dato anche attraverso modalità diverse da quelle logiche, è necessario predisporre le opportune misure di protezione di natura fisica, sia di tipo preventivo che di monitoraggio;
- le misure di protezione fisica riguardano primariamente l'area in cui sono presenti i sistemi IT, riguardano prioritariamente la protezione dei varchi dell'edificio e l'ausilio aggiuntivo di sistemi di videosorveglianza.

5. Copie 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.

Non duplica integralmente o parzialmente dati dell'Amministrazione se non per i suddetti motivi.

Il Responsabile esterno, alla scadenza del Contratto o, comunque, in caso di cessazione per qualunque causa dell'efficacia della nomina a Responsabile esterno, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario che preveda la conservazione dei dati

personali, provvede, a scelta dell'Amministrazione, all'immediata restituzione dei dati personali oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente un'attestazione scritta che non ne esiste alcuna copia presso lo stesso. Il Responsabile esterno fornisce assicurazione che allo stesso comportamento si sono adeguati i sub-Responsabili dallo stesso nominati. In caso di richiesta scritta dell'Amministrazione, il Responsabile esterno è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione dei dati.