ALLEGATO

al *Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. i) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del Codice dell'amministrazione digitale*

MODALITÀ DI ESECUZIONE DELLE VERIFICHE SUI SOGGETTI VIGILATI

INDICE

1 DEFINIZIONI 3
2 PREMESSA 4
3 OBIETTIVI DELLE VERIFICHE 4
4 PROGRAMMAZIONE DELLE VERIFICHE 4
5 DOCUMENTI DI RIFERIMENTO E METODI DI RISCONTRO 5
5.1 DOCUMENTI DI RIFERIMENTO A CARICO DEL SOGGETTO VIGILATO 5
5.2 DOCUMENTI DI RIFERIMENTO E STRUMENTI DI SUPPORTO PER IL VERIFICATORE 6
6 IL PROCESSO PER L'ESECUZIONE DELLE VERIFICHE ISPETTIVE 7
6.1 PREPARAZIONE DELLA VERIFICA 7
6.2 ESECUZIONE DELLA VERIFICA 8
6.2.1 CLASSIFICAZIONE DEI RILIEVI 9
6.3 DOCUMENTAZIONE DEI RISULTATI E AZIONI CONSEGUENTI 9
7 GESTIONE DELLE COMUNICAZIONI E DELLA DOCUMENTAZIONE 9

1 DEFINIZIONI

Ai fini del presente documento si applicano le definizioni indicate all'art. 1 del "Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. i) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-*bis* del d. lgs. 7 marzo 2005, n. 82 e successive modificazioni". Si applicano, inoltre, le seguenti:

CAB: Conformity Assessment Body – Organismo di certificazione di conformità accreditato da ACCREDIA o da altro ente di Accreditamento rientrante nell'ambito del Regolamento (CE) N. 2008/765, firmatario degli accordi di Mutuo riconoscimento nello schema specifico.

CAR: Conformity Assessment Report – relazione di confromità rilasciata da un CAB.

evidenze: registrazioni, dichiarazioni di fatti o altre informazioni che sono pertinenti agli obiettivi delle verifiche e sono verificabili.

Regolamento: "Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. i) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del d. lgs. 7 marzo 2005, n. 82 e successive modificazioni".

2 PREMESSA

In relazione alle previsioni indicate all'art. 14-bis, comma 2, lettera i) del Codice dell'Amministrazione Digitale l'Agenzia per l'Italia Digitale svolge funzioni di "*Vigilanza sui servizi fiduciari ai sensi dell'articolo 17 del regolamento UE 910/2014 in qualità di organismo a tal fine designato, sui gestori di posta elettronica certificata, sui soggetti di cui all'articolo 34, comma 1-bis, lettera b), nonché sui soggetti pubblici e privati, che partecipano a SPID di cui all'articolo 64; nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'articolo 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza*".

Ai prestatori dei servizi di cui sopra, sottoposti alle attività di vigilanza, si applicano specifiche norme tecniche che, insieme alle norme sopra richiamate, definiscono gli obblighi dei gestori nell'erogazione dei servizi previsti.

A prescindere dalle caratteristiche di ciascuna tipologia di servizio, le verifiche per l'espletamento della vigilanza sono condotte secondo modalità definite, descritte nel presente documento. La disciplina per l'espletamento dell'attività pre-istruttoria di verifica e per l'irrogazione delle sanzioni previste all'art. 32-bis del CAD è oggetto del Regolamento.

3 OBIETTIVI DELLE VERIFICHE

Le funzioni di vigilanza sono volte a: verificare che i soggetti vigilati ed i servizi da essi prestati rispondano nel tempo ai requisiti previsti dalla disciplina di riferimento; accertare violazioni o irregolarità; rilevare situazioni potenzialmente critiche; favorire il miglioramento continuo dei processi di erogazione dei servizi.

Situazioni frequenti di irregolarità, procedure o regole disattese o scostamenti ripetuti rispetto ai livelli di prestazioni previsti sono indice di degrado del processo del fornitore o delle capacità tecniche dimostrate in fase di qualificazione e, nei casi in cui siano commesse le violazioni previste dall'art. 32-bis del CAD, comportano l'attivazione di procedimenti sanzionatori, secondo le modalità descritte nel Regolamento.

4 PROGRAMMAZIONE DELLE VERIFICHE

Le verifiche documentali sono svolte in via continuativa e prendono in esame la documentazione di riscontro prevista nelle norme di riferimento per ciascun servizio.

Le verifiche ispettive sono programmate in linea generale con frequenza quadrimestrale. Il programma è predisposto sulla base di un profilo di rischio del soggetto vigilato determinato su più elementi che, a titolo non esaustivo, includono:

- risultati delle verifiche condotte sui documenti di riferimento;
- dimensioni e tipologia di servizi e utenti;
- dati di riepilogo sui servizi erogati;

- soluzioni tecnologiche adottate;
- *partner* che gestiscono specifiche componenti di servizio;
- notifiche relative a disservizi o violazioni di sicurezza o perdita di integrità o interruzioni di servizio;
- segnalazioni o richieste da utenti, altri operatori, amministrazioni o autorità nazionali;
- richieste da altri organismi di vigilanza o istituzioni europee (per quanto riguarda i servizi fiduciari qualificati);
- esiti di verifiche precedenti.

Tali elementi concorrono ad inquadrare i soggetti vigilati per ciascun ambito in una matrice aggiornata nel tempo, che attribuisce ad ogni soggetto vigilato/ambito un indice di rischio.

Le verifiche possono essere disposte anche in via estemporanea, a fronte di eventi o situazioni contingenti, quali segnalazioni o richieste pervenute da utenti o organizzazioni esterne o analisi effettuate su fonti pubbliche.

Per l'esecuzione delle attività ispettive AgID può incaricare soggetti terzi, nell'ambito di appositi accordi o contratti stipulati per tali finalità.

Il processo per la conduzione delle verifiche ispettive è descritto al § 6.

Nell'ambito delle attività programmate, possono essere condotte verifiche attraverso la somministrazione, anche attraverso piattaforma informatica, di questionari o liste di riscontro che, a seconda di specifiche esigenze funzionali alle attività di vigilanza, uno o più soggetti vigilati sono tenuti a compilare in modalità "*self-assessment*" nei termini a tal fine comunicati.

5 DOCUMENTI DI RIFERIMENTO E METODI DI RISCONTRO

5.1 DOCUMENTI DI RIFERIMENTO A CARICO DEL SOGGETTO VIGILATO

Le verifiche documentali sono condotte con riferimento alla seguente documentazione:

a. documenti depositati presso AgID ai fini della qualificazione o dell'accreditamento o al fine di dimostrare il possesso dei requisiti di qualità, sicurezza, organizzazione o di analoga fattispecie previsti dal CAD, indicati nelle norme di riferimento per ciascun servizio e ogni successivo aggiornamento a fronte di modifiche intervenute, che il soggetto vigilato è obbligato a trasmettere ai sensi della stessa normativa.

b. documenti di riscontro indicati nelle norme. A titolo di esempio:
   1. CAR biennali, se previsti;
   2. piani di cessazione (art. 24, par. 2, lett. i) del Regolamento eIDAS)
   3. rapporti periodici di riepilogo delle attività svolte;

4. certificati di conformità agli standard internazionali quali ISO/IEC 27001, ISO 9001 previsti ai fini della qualificazione o accreditamento, e documentazione contenente le risultanze delle verifiche periodiche di mantenimento;
5. ogni altro documento correlato all'espletamento dei processi di erogazione dei servizi che AgID ha facoltà di richiedere;

c. registrazioni di attività svolte in esecuzione delle procedure indicate nei manuali (Manuale operativo, Piano della sicurezza) e nell'ulteriore documentazione relativa ai sistemi utilizzati per l'erogazione dei servizi. Dette registrazioni, a titolo di esempio, includono:

1. risultati generati dai processi, svolti secondo le procedure previste nell'ambito della documentazione del sistema. Tali risultati possono consistere in documenti, aggiornamenti di archivi, verbali;
2. documenti contenenti i risultati di verifiche ispettive interne o di audit di terza parte se previste dai sistemi di gestione della qualità e dai sistemi di gestione della sicurezza adottati dal soggetto vigilato;
3. ogni documento che dimostri l'effettiva e corretta applicazione, nel tempo, dei sistemi, delle regole e delle procedure definite per l'erogazione dei servizi a norma.

5.2 DOCUMENTI DI RIFERIMENTO E STRUMENTI DI SUPPORTO PER IL VERIFICATORE

Il verificatore effettua le verifiche documentali e le verifiche ispettive basandosi sulla documentazione di cui al § 5.1.

Costituiscono, inoltre, parametri per le valutazioni del verificatore il complesso delle norme e degli standard di riferimento per ciascun servizio, indicati nelle norme specialistiche o anche *de facto*, con le relative evoluzioni nel tempo.

Per l'esecuzione delle verifiche, il verificatore può utilizzare apposite liste di riscontro (*check list*), contenenti i principali requisiti previsti dalle norme di riferimento rispetto a cui sono condotte le valutazioni.

6 IL PROCESSO PER L'ESECUZIONE DELLE VERIFICHE ISPETTIVE

Le verifiche ispettive sono condotte di regola secondo i principi della norma UNI EN ISO 19011. In Fig. 7.a si rappresenta uno schema del processo di verifica, articolato in tre fasi principali, descritte nei paragrafi che seguono.

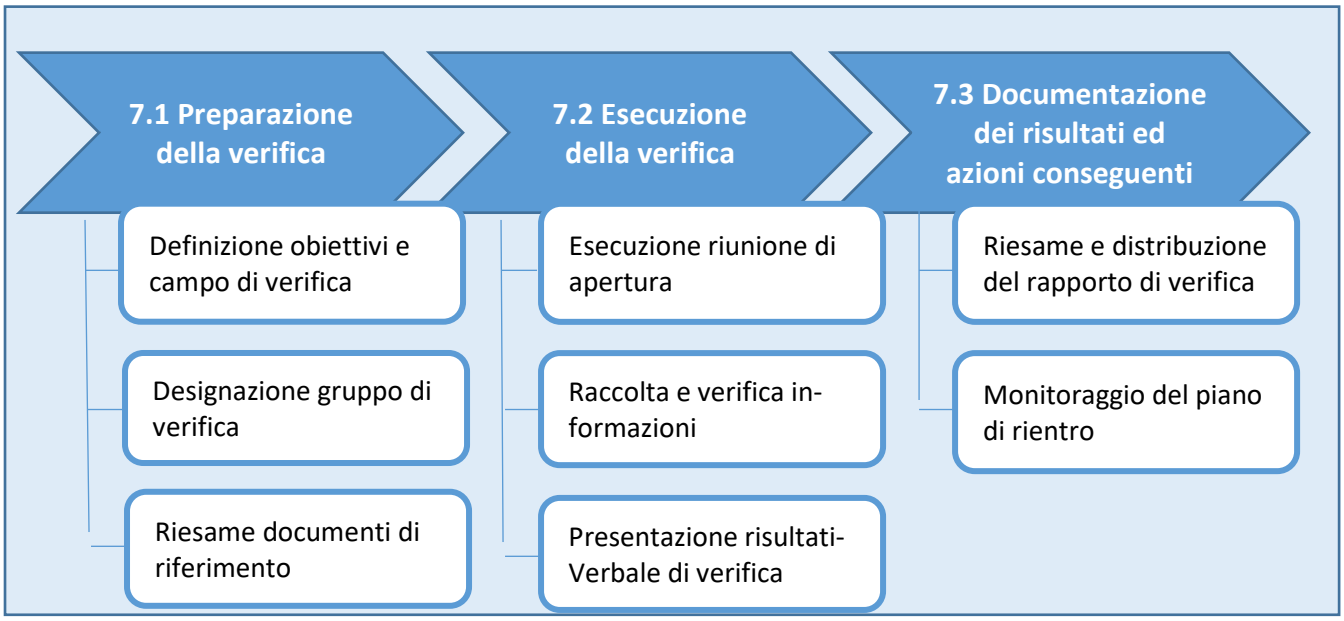

Fig. 7.a – *Processo di verifica ispettiva*

6.1 PREPARAZIONE DELLA VERIFICA

Per ciascuna verifica ispettiva, programmata o disposta in via estemporanea, si predispone, a seguito dell'esame preliminare della documentazione di riferimento, un piano di verifica.

Il piano indica:

a. obiettivi e campo della verifica (elementi del sistema o componenti dei servizi o prodotti che saranno oggetto di verifica);

b. documenti di riferimento e tipologie di documenti di riscontro che dovranno essere esibiti nel corso della visita, con riferimento alle tipologie previste al § 5.1;

c. data di inizio delle attività di verifica e modalità di svolgimento;

d. stima del tempo e della durata delle attività;

e. composizione del gruppo di verifica, con indicazione di eventuali accompagnatori.

La composizione del gruppo di verifica è stabilita in funzione degli obiettivi e del campo della verifica. A tal fine può essere prevista la partecipazione di personale di unità organizzative AgID con specifiche competenze (ad esempio in materia di sicurezza, di infrastrutture di rete, di protezione tecnica dei sistemi e

delle applicazioni, ecc.) nel ruolo di esperti tecnici e la partecipazione di personale di amministrazioni/autorità esterne nei casi previsti dalle norme di riferimento o nell'ambito di specifici accordi o contratti stipulati dall'Agenzia.

Il piano di verifica è trasmesso al Gestore almeno 24 ore prima della data prevista di inizio delle attività di verifica. In casi particolari di gravità o urgenza, a discrezione di AgID, il piano di verifica può essere comunicato con tempi inferiori di preavviso.

A completamento della fase di preparazione, il gruppo di verifica predispone i documenti di lavoro, che possono comprendere liste di riscontro, piani di campionamento e moduli per la registrazione delle informazioni, delle risultanze della verifica e delle riunioni.

6.2 ESECUZIONE DELLA VERIFICA

La verifica può essere condotta *on site*, da remoto o in combinazione e si svolge secondo i tempi indicati nel piano di verifica, di cui al 6.1. I partecipanti sono identificati e l'inizio delle attività è ufficializzato in un incontro del gruppo di verifica con un Responsabile del soggetto sottoposto a verifica o con persona da questi formalmente incaricata; ove appropriato, a discrezione del Responsabile, partecipano all'incontro i responsabili delle funzioni o dei processi da sottoporre a verifica.

Lo scopo della riunione di apertura è di riepilogare il piano, fornire una breve sintesi di come verranno eseguite le attività, confermare i canali di comunicazione.

Nel corso della verifica si provvede a raccogliere e verificare le informazioni. I metodi per raccogliere informazioni comprendono:

- interviste;
- compilazione di liste di riscontro/formulari anche da parte dei partecipanti;
- raccolta di documentazione;
- osservazioni di attività e acquisizione di *screenshot*;
- rilevazione evidenze;
- analisi delle registrazioni di sistema (es. log; configurazioni di prodotti software, ecc.).

Della seduta di verifica è redatto un verbale ("Verbale di verifica"), condiviso e firmato digitalmente al termine della seduta stessa. Tutti i documenti esibiti nel corso della seduta sono raccolti in un archivio .zip opportunamente cifrato per assicurare l'integrità, l'autenticità, il non ripudio, la tracciabilità e la confidenzialità; tali documenti sono depositati come allegati al verbale.

Le informazioni acquisite nel corso della verifica, il verbale e la relativa documentazione sono utilizzati per la redazione del Rapporto di Verifica di cui all'art. 4, comma 4, del Regolamento.

Nel caso in cui la verifica è condotta da remoto, il Gestore deve attenersi alle indicazioni fornite nel piano di verifica di cui al § 6.1, che includono almeno le seguenti condizioni:

- durante la sessione di verifica, camera sempre accesa e ambiente isolato;
- microfono attivo solo per la persona intervistata;
- utilizzo della funzione "alza mano" per richiedere la parola;

- accesso ai sistemi da remoto mediante un operatore eventualmente in presenza presso la sede operativa del Gestore.

A conclusione delle attività, si presentano le risultanze e le conclusioni della verifica. Sono discusse e, se possibile risolte, eventuali divergenze di opinione e, in caso di mancato accordo, tutte le opinioni sono registrate nel verbale.

6.2.1 CLASSIFICAZIONE DEI RILIEVI

I rilievi possono derivare sia da verifiche svolte su base documentale, anche a seguito di segnalazioni, sia dalle verifiche ispettive. Sono distinti in "Osservazione" e "Non Conformità", queste ultime classificate secondo livelli di gravità decrescente. Il Regolamento disciplina le modalità per la classificazione e gestione dei rilievi.

6.3 DOCUMENTAZIONE DEI RISULTATI E AZIONI CONSEGUENTI

Il rapporto di verifica fornisce una completa registrazione delle attività svolte. Include o fa riferimento, quando appropriato, a:

a. piano della verifica;
b. elenco dei rappresentanti dell'organizzazione oggetto di verifica;
c. elenco della documentazione esaminata;
d. sintesi del processo di verifica comprendente incertezze o eventuali ostacoli incontrati;
e. eventuali aree non coperte;
f. eventuali opinioni divergenti non risolte tra il gruppo di verifica e l'organizzazione ed eventuali dichiarazioni del Gestore;
g. eventuali osservazioni e non conformità;
h. eventuali piani delle azioni successive.

Il rapporto di verifica è notificato al Gestore come previsto all'art. 4, comma 4, del Regolamento. In caso di osservazioni o non conformità, il Gestore procede come previsto agli artt. 5 e 6 del Regolamento.

Il completamento e l'efficacia delle azioni correttive e delle ulteriori azioni preventive o migliorative possono costituire oggetto di una nuova verifica.

7 GESTIONE DELLE COMUNICAZIONI E DELLA DOCUMENTAZIONE

Le comunicazioni finalizzate all'esecuzione delle verifiche e la trasmissione dei documenti a carico del Gestore sono effettuate a mezzo PEC o altro servizio elettronico di recapito certificato qualificato di cui all'art.1, comma 1-ter del CAD, salvo i casi di documenti che non possono essere divulgati all'esterno dell'organizzazione e che sono consultabili presso il Gestore. La trasmissione dei documenti in formato

elettronico è eseguita secondo le procedure definite dal Gestore per la protezione dei dati e delle informazioni, ovvero secondo le indicazioni fornite da AgID per la trasmissione di documenti riservati.