MISSIONE 1 – IL PIANO NAZIONALE RIPRESA E RESILIENZA (PNRR) E LA CYBERSICUREZZA - Il D.Lgs. 3 agosto 2022, n. 123 e l'attuazione del quadro per l'introduzione di sistemi europei di certificazione (*Appendice II*)

PNRR

Dossier

Sommario

1. Premessa

Con il D.Lgs. 3 agosto 2022, n. 123 (entrato in vigore il 4 settembre 2022) sono state emanate le norme di attuazione del c.d. *Cybersecurity Act* Europeo, il Regolamento (Ue) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'*Agenzia dell'Unione europea per la cybersicurezza*, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (*regolamento sulla cybersicurezza*).

La normativa euro unitaria persegue come finalità principale quella di garantire *il buon funzionamento del mercato interno perseguendo allo stesso tempo un elevato livello di cybersicurezza, cyberesilienza e fiducia all'interno dell'Unione*. A tal fine detto Regolamento stabilisce:

a) gli *obiettivi*, i *compiti* e gli *aspetti organizzativi* relativi all'ENISA, (*Agenzia dell'Unione europea per la cybersicurezza*);

b) un *quadro per l'introduzione di sistemi europei di certificazione della cybersicurezza* al fine di garantire un livello adeguato di cybersicurezza dei prodotti TIC[1], servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cybersicurezza nell'Unione.

Rispetto alla disciplina dell'ENISA il Regolamento mira ad emancipare l'Agenzia dal ruolo di mera assistenza tecnica alle Istituzioni europee e agli Stati membri nella predisposizione delle politiche in materia di sicurezza informatica per attribuirle anche un ruolo attivo nella gestione operativa degli incidenti informatici.

La definizione di un *corpus* normativo europeo comune in materia di certificazione della sicurezza delle Tecnologie dell'Informazione e della Comunicazione (prodotti, servizi e processi informatici) consente un approccio armonizzato dei sistemi europei di certificazione della cybersicurezza fornendo regole comuni in materia di disponibilità, autenticità, integrità e la riservatezza dei dati processati (conservati, trattati, e trasmessi) e dei servizi offerti *on-*

[1] L'acronimo TIC sta ad indicare prodotti, servizi e processi realizzati attraverso la Tecnologia dell'Informazione e della Comunicazione.

line. La disciplina comune europea in materia di certificazione della cybersicurezza trova applicazione in materia di certificazione sia volontaria che obbligatoria.

2. Il D.Lgs. 3 agosto 2022, n. 123: funzione ed ambito di applicazione

Il D.Lgs. n. 123/2022 individua le misure necessarie per adeguare la normativa interna al *nuovo quadro europeo di certificazione della cybersicurezza*, introdotto mediante le disposizioni del Titolo III del citato Regolamento (UE) 2019/881.

A tal fine, il D.Lgs. n. 123/2022 prevede:

a) l'individuazione dell'organizzazione dell'*Autorità nazionale di certificazione della cybersicurezza* in Italia, di cui all'articolo 4, comma 1, in base ai compiti ed ai poteri ad essa attribuiti in materia di vigilanza in ambito nazionale e di rilascio dei certificati di *cybersicurezza*, con riferimento al quadro europeo di certificazione;

b) le modalità di cooperazione dell'*Autorità nazionale di certificazione della cybersicurezza* italiana con le altre autorità pubbliche nazionali ed europee e con l'*Organismo di accreditamento*[2];

c) la definizione di un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione con sanzioni effettive, proporzionate e dissuasive.

La disciplina di attuazione del quadro per l'introduzione di sistemi europei di certificazione di cui al D.Lgs. n. 123/2022 trova applicazione generale ma restano salve le disposizioni specifiche riguardanti le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.

[2] L'art. 3, comma 1, lett. m) del D.Lgs. n. 123/2022 definisce l'*Organismo di accreditamento* come l'organismo autorizzato a svolgere l'attività di accreditamento nel territorio dello Stato, ai sensi dell'art. 2, par. 1, n. 11, del Regolamento (CE) 765/2008, designato con decreto del Ministro dello sviluppo economico del 22 dicembre 2009 in attuazione dell'articolo 4, comma 2, della legge 23 luglio 2009, n. 99. A tal proposito si ricorda che secondo quanto previsto dal precedente n. 10, dell'art. 2, par. 1, del Regolamento (CE) 765/2008, per *accreditamento* deve intendersi l'*attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità*.

Rispetto all'applicazione di questa disciplina l'art. 2 chiarisce che il trattamento dei dati personali derivante dall'applicazione del D.Lgs. n. 123/2022 è effettuato ai sensi del *Regolamento Generale sulla Protezione dei Dati* GDPR (Regolamento (UE) 2016/679) e del c.d. *Codice della privacy* di cui al D.Lgs. 30 giugno 2003, n. 196.

3. La Vigilanza nazionale

L'*Agenzia per la cybersicurezza nazionale*, ai sensi dell'art. 5, realizza l'attività di vigilanza del mercato in ambito nazionale ai fini della corretta applicazione delle regole previste dai sistemi europei di certificazione della *cybersicurezza*, con riferimento ai certificati di *cybersicurezza* ed alle dichiarazioni UE di conformità emessi nel territorio dello Stato nel rispetto della normativa interna ed euro unitaria. A tal fine essa vigila su fornitori e fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di *cybersicurezza* e sugli organismi di valutazione della conformità[3]. In quest'ambito l'*Agenzia per la cybersicurezza nazionale*:

a) assiste e sostiene attivamente l'*Organismo di accreditamento* nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità[4]. Le modalità di sostegno ed assistenza dell'Agenzia all'*Organismo di accreditamento* per l'attività di vigilanza sono disciplinate da apposita convenzione o protocollo di intesa fra i medesimi soggetti;

b) monitora e vigila sulle attività degli organismi di valutazione della conformità pubblici di cui all'art. 56, par. 5, lett. b), del Regolamento (UE) 2019/881[5];

c) ove previsto dal sistema di certificazione, autorizza gli organismi di valutazione della conformità e limita, sospende o revoca l'autorizzazione esistente qualora violino le

[3] L'Agenzia, per le prove tecniche nell'ambito delle attività di vigilanza nazionale, può effettuare valutazioni di sicurezza informatica anche attraverso esperti esterni o laboratori di prova abilitati dall'Agenzia e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

[4] Resta, comunque, salvo quanto previsto dall'art. 60, par. 3, del Regolamento (UE) 2019/881 per le ipotesi in cui i sistemi europei di certificazione della cybersicurezza stabiliscono requisiti specifici o supplementari nonché quanto previsto dalle disposizioni in materia di funzioni di monitoraggio e vigilanza sulle attività degli organismi di valutazione.

[5] La norma in questione prevede che in casi debitamente giustificati, un sistema europeo di certificazione della cybersicurezza può prevedere che i certificati europei di cybersicurezza derivanti da tale sistema possano essere rilasciati unicamente da un ente pubblico. Detto ente può essere, alternativamente, uno dei due soggetti seguenti:

a) un'autorità nazionale di certificazione della cybersicurezza designata ai sensi dell'art. 58, par. 1, del Regolamento (UE) 2019/881, oppure un'autorità nazionale di certificazione della cybersicurezza stabilita in un altro Stato membro designata, a seguito di accordo con lo stesso Stato, affinché sia responsabile dei compiti di vigilanza;
b) un organismo pubblico accreditato come organismo di valutazione della conformità a norma dell'articolo 60, paragrafo.

prescrizioni del Regolamento medesimo, dandone notizia all'Organismo di accreditamento.

L'Agenzia, nello svolgimento dell'attività di vigilanza, opera anche in collaborazione con altre autorità di vigilanza del mercato competenti in Italia e con le autorità di vigilanza degli altri Stati membri[6]. L'Agenzia esegue l'attività di vigilanza anche in collaborazione con le Forze dell'ordine.

Nell'attività di vigilanza affidatale, l'Agenzia può effettuare, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di *cybersicurezza* e degli emittenti le dichiarazioni di conformità UE, indagini ed *audit*, ottenendo informazioni anche tramite l'accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di *cybersicurezza*, revocare certificati, irrogare sanzioni pecuniarie ed accessorie. L'attività di vigilanza dell'Agenzia può prevedere prelievi di prodotti.

Nel caso in cui l'Agenzia, in esito alle attività di vigilanza, accerti l'emissione di un certificato non conforme, rilasciato ai sensi del Regolamento (UE) 2019/881[7], detto certificato è sottoposto a revoca:

a) per il livello di affidabilità *elevato* l'Agenzia provvede direttamente alla revoca del certificato;

b) per il livello di affidabilità di *base* o *sostanziale* nel caso in cui il certificato non conforme sia relativo ad un prodotto TIC, servizio TIC o processo TIC che ha comportato un concreto e dimostrato pregiudizio ad un servizio essenziale, ad un servizio di comunicazione elettronica, alla salute o all'incolumità personale l'Agenzia chiede all'organismo che ha emesso il certificato di provvedere alla revoca del

[6] Come individuate dall'art. 58, par. 7, lett. a) ed h), del Regolamento (UE) 2019/881.

[7] Il riferimento è ai certificati rilasciati ai sensi dell'art. 56, par. 4, 5, lett. b), o 6, lettere a) e b), del Regolamento (UE) 2019/881. Nello specifico, il par. 4 individua due categorie di certificati, in base al livello di affidabilità, qualificati come «*di base*» o «*sostanziale*». Tale classificazione è operata sulla base dei criteri previsti dal sistema europeo di certificazione della cybersicurezza. Il successivo paragrafo 5, lett. b), derogando parzialmente i principi di cui al comma precedente prevede che, in casi debitamente giustificati, un sistema europeo di certificazione della cybersicurezza possa prevedere che i certificati europei di cybersicurezza possano essere rilasciati unicamente da un organismo pubblico accreditato come organismo di valutazione della conformità. Infine, il sesto comma dispone che, ove un sistema europeo di certificazione della cybersicurezza richieda un livello di affidabilità «*elevato*», il certificato europeo di cybersicurezza nell'ambito di tale sistema deve essere rilasciato solo da un'autorità nazionale di certificazione della cybersicurezza oppure, nei casi seguenti, da un organismo di valutazione della conformità:

a) previa approvazione dell'autorità nazionale di certificazione della cybersicurezza per ogni singolo certificato europeo di cybersicurezza rilasciato da un organismo di valutazione della conformità;
b) sulla base di una delega generale del compito di rilasciare tali certificati europei di cybersicurezza a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cybersicurezza.

certificato entro e non oltre cinque giorni e, in caso di inottemperanza, provvede direttamente entro i successivi cinque giorni;

c) se previsto espressamente dallo specifico sistema europeo di certificazione, si provvede in base alle regole stabilite dal sistema specifico di certificazione.

Accertata l'emissione di un certificato non conforme, in esito alle attività e fatti salvi i casi di revoca testé illustrati, l'Agenzia chiede all'organismo che ha emesso il certificato di ripetere in tutto o in parte l'attività di valutazione o di integrare tale attività con ulteriori verifiche e, quindi, di ricondurre il certificato a conformità entro centoventi giorni o revocare il certificato. In caso di mancata riconduzione a conformità o mancata revoca del certificato non conforme da parte dell'organismo, il certificato decade. La riconduzione a conformità o la revoca del certificato sono divulgate con gli strumenti e le modalità previsti dal sistema europeo di certificazione della cybersicurezza nell'ambito della propria la politica di divulgazione dei certificati europei di cybersicurezza rilasciati, modificati o revocati nell'ambito del sistema.

L'attavo comma dell'art. 5 obbliga gli organismi di valutazione della conformità, i titolari dei certificati europei di cybersicurezza e gli emittenti delle dichiarazioni di conformità durante l'attività di vigilanza a cui sono sottoposti a cooperare con l'Agenzia nell'attività di verifica sui certificati e sulle dichiarazioni UE da essi emessi. A tal fine detti soggetti, su richiesta dell'Agenzia, devono mettere a disposizione tutti i documenti di valutazione necessari per dimostrare la conformità dei certificati e le dichiarazioni oggetto di verifica da parte dell'Agenzia assieme agli strumenti di valutazione eventualmente forniti dal fabbricante o dal fornitore nell'attività di valutazione come indicato nei rapporti di valutazione. L'onere della prova della conformità di certificati e dichiarazioni è in capo agli organismi di valutazione della conformità, ai titolari dei certificati o agli emittenti delle dichiarazioni di conformità.

4. Il Rilascio dei certificati di cybersicurezza

I certificati di cybersicurezza vengono inquadrati in una classificazione tripartita, in ragione del livello di affidabilità:

- *affidabilità di base* quanto il certificato garantisce che un prodotto TIC, servizio TIC o processo TIC è stato oggetto di valutazione ad un livello comunque sufficiente a ridurre i rischi legati ai più diffusi incidenti o attacchi informatici;
- *affidabilità sostanziale* quando il certificato garantisce l'esistenza di standard e funzionalità di sicurezza elevati, tali da limitare i rischi noti di attacchi informatici causati da soggetti dotati di abilità e risorse limitate;
- *affidabilità elevata* quando il certificato assicura che un prodotto TIC, servizio TIC o processo TIC rispetta i requisiti di sicurezza e sia stato oggetto di valutazioni mirate alla minimizzazione dei rischi derivanti da attacchi informatici.

L'Agenzia, ai sensi dell'art. 6, D.Lgs. n. 123/2022, rilascia i certificati di cybersicurezza con livello di affidabilità *elevato* tramite l'*Organismo di Certificazione della Sicurezza Informatica* (OCSI), che si può avvalere di esperti o di laboratori di prova abilitati dall'Agenzia ad operare per proprio conto e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale, ferme restando, per specifici sistemi di certificazione, le possibili modalità di emissione dei certificati alternative (ai sensi dell'art. 56, par. 6, lettere a) e b), del Regolamento, che individuano le fattispecie in cui un sistema europeo di certificazione della cybersicurezza può richiedere un livello di affidabilità «*elevato*).

Ove uno specifico sistema di certificazione preveda il rilascio dei certificati con livello di affidabilità *sostanziale* o *di base* unicamente da parte di un organismo pubblico, l'Agenzia rilascia tali certificati attraverso l'OCSI. Il rilascio può avvenire ad opera di altro organismo di valutazione della conformità pubblico, accreditato dall'*Organismo di Accreditamento*, monitorato e vigilato dall'Agenzia nel rispetto della normativa euro unitaria e designato dall'Agenzia con proprio provvedimento, salvo diverse disposizioni dello specifico sistema europeo di certificazione.

La certificazione della cybersicurezza è volontaria, salvo il caso in cui sia diversamente specificato dal diritto dell'Unione o dal diritto nazionale. In mancanza di un diritto dell'Unione armonizzato, l'Agenzia può adottare, previa consultazione con i portatori di interesse, regolamentazioni tecniche nazionali in cui sia prevista una certificazione obbligatoria nel quadro di un sistema europeo di certificazione della cybersicurezza (art. 6, comma 3).

Gli oneri legati al rilascio dei certificati da parte dell'Agenzia sono a carico del soggetto richiedente la certificazione.

5. Le dichiarazioni UE di conformità

In un sistema di certificazione in cui è autorizzata l'*autovalutazione di conformità* i fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC possono rilasciare sotto la propria responsabilità dichiarazioni UE di conformità di livello di base per dimostrare il rispetto di requisiti tecnici previsti nel sistema (art. 7).

Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC rende disponibile all'Agenzia, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cybersicurezza:

- la dichiarazione UE di conformità;
- la documentazione tecnica;
- tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC o servizi TIC al sistema.

Una copia della dichiarazione UE di conformità è, inoltre, trasmessa all'Agenzia e all'ENISA.

Nel caso in cui l'Agenzia, in esito alle attività di vigilanza, accerti la non conformità di una dichiarazione UE di conformità sorge in capo al fabbricante (o al fornitore o emittente) l'obbligo di revisionare o revocare la dichiarazione stessa entro trenta giorni, dandone comunicazione all'Agenzia e all'ENISA, salvo diversa disposizione dello specifico sistema di certificazione.

Il quarto comma dell'art. 7 ribadisce il principio di cui all'art. 53, par. 4 del Regolamento (UE) 2019/881 secondo cui il rilascio di una dichiarazione UE di conformità è volontario, salvo in caso in cui sia diversamente specificato dalla normativa interna o da quella europea. In mancanza di un diritto dell'Unione armonizzato, l'Agenzia può stabilire, previa consultazione con i portatori di interesse, l'obbligatorietà della dichiarazione UE di conformità nelle fattispecie di cui all'art. 6, comma 3 (cfr. *supra*).

6. L'accreditamento e l'autorizzazione degli organismi di valutazione della conformità e l'abilitazione dei laboratori di prova ed esperti dell'Agenzia

Ai sensi dell'art. 8, comma 1 del D.Lgs. n. 123/2022, l'*Organismo di accreditamento*, nello svolgimento dei compiti relativi all'accreditamento degli organismi di valutazione della conformità e dell'autorità nazionale di certificazione (di cui ai par. 1, 2 e 4 dell'art. 60 del Regolamento (UE) 2019/881), ed in conformità con le disposizioni dello specifico sistema di certificazione, comunica all'Agenzia ed all'*Ufficio unico di collegamento designato per l'Italia*[8], ogni aggiornamento in merito agli organismi di valutazione della conformità accreditati quanto a nuovi rilasci, revoche, sospensioni e limitazioni dei certificati di accreditamento per la successiva notifica da parte dell'Agenzia alla Commissione europea. L'Agenzia partecipa con propri rappresentanti alle deliberazioni dell'*Organismo di accreditamento* in ordine allo svolgimento di tali attività.

Qualora un sistema europeo di certificazione stabilisca, conformemente alle previsioni di cui dell'art. 54, par. 1, lettera f), del Regolamento (UE) 2019/881, requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione della conformità al fine di garantire che abbiano la competenza tecnica per valutare i requisiti di cybersicurezza, solo gli organismi di valutazione della conformità che soddisfano detti requisiti sono autorizzati dall'Agenzia a svolgere i compiti previsti da tale sistema.

In relazione alle attività di vigilanza nazionale e di rilascio dei certificati, l'Agenzia, con provvedimento adottato secondo la descritta procedura di cui all'art. 5, comma 3, del D.P.C.M. n. 223/2021 (cfr. *supra*), costituisce, aggiorna e rende pubblici due elenchi di esperti e di laboratori di prova da essa abilitati ad operare rispettivamente a supporto delle attività di vigilanza e rilascio dei certificati in capo all'Agenzia. Gli esperti e i laboratori di prova inseriti nell'elenco dei soggetti abilitati, iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale (di cui all'art. 5, comma 7 del D.Lgs. 123/2022), non possono effettuare attività di valutazione per l'emissione di certificati con livello di affidabilità *sostanziale* o *di base* in ambito nazionale, né possono essere accreditati come organismi di valutazione della conformità per il rilascio di tali certificati. Con la medesima procedura testé

[8] Ai sensi dell'art. 10, par. 3, del Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, *sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011*, ogni Stato membro designa un ufficio unico di collegamento. La designazione, quindi avviene ad opera dello stesso Stato membro.

richiamata, sono individuate le modalità per l'abilitazione e l'eventuale rinnovo, l'inserimento, la sospensione e la cancellazione di esperti e laboratori di prova dai suddetti elenchi.

Gli oneri derivanti dall'abilitazione, le spese per le eventuali attività di autorizzazione e gli eventuali successivi aggiornamenti, conformemente all'art. 30, commi 4 e 5, della L. 24 dicembre 2012, n. 234[9],sono a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione.

7. L'attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della *cybersicurezza*

L'agenzia può realizzare progetti di ricerca al fine di elevare il livello nazionale di *cybersicurezza*. Rientrano in quest'ambito anche i progetti per lo sviluppo di *software* e di formazione, anche in collaborazione con università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica, anche nel contesto di attività di supporto alla standardizzazione a livello nazionale, europeo ed internazionale (art. 9).

L'Agenzia monitora gli sviluppi nel campo della certificazione della *cybersicurezza*, anche consultando i portatori di interesse nazionale del settore e scambiando informazioni, esperienze e buone pratiche con la Commissione europea e le altre autorità nazionali della *cybersicurezza*.

Conformemente all'articolo 57 del Regolamento (UE) 2019/881 ed in assenza di un sistema europeo di certificazione, *l'Agenzia può introdurre sistemi di certificazione nazionali della cybersicurezza, per prodotti TIC, servizi TIC o processi TIC.*

[9] In particolare, i commi 4 e 5, dell'art. 30, L. 24 dicembre 2012, n. 234 *Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea* prevedono che:
[...]
4. Gli oneri relativi a prestazioni e a controlli da eseguire da parte di uffici pubblici, ai fini dell'attuazione delle disposizioni dell'Unione europea di cui alla legge di delegazione europea per l'anno di riferimento e alla legge europea per l'anno di riferimento, sono posti a carico dei soggetti interessati, ove ciò non risulti in contrasto con la disciplina dell'Unione europea, secondo tariffe determinate sulla base del costo effettivo del servizio reso. Le tariffe di cui al primo periodo sono predeterminate e pubbliche.
5. Le entrate derivanti dalle tariffe determinate ai sensi del comma 4 sono attribuite, nei limiti previsti dalla legislazione vigente, alle amministrazioni che effettuano le prestazioni e i controlli, mediante riassegnazione ai sensi del regolamento di cui al decreto del Presidente della Repubblica 10 novembre 1999, n. 469.

8. Il sistema sanzionatorio

L'art. 10 prevede che l'Agenzia, in caso di violazione degli obblighi del quadro europeo di certificazione della cybersicurezza, irroghi sanzioni pecuniarie ed accessorie, chiedendo la cessazione immediata della violazione. Si applica, in quanto compatibile, la disciplina generale in materia di sanzioni amministrative di cui alla legge 24 novembre 1981, n. 689[10].

L'art. 10 contiene una lunga elencazione di fattispecie per le quali individua, nel minimo e nel massimo la sanzione amministrativa applicabile. Nello specifico, salvo che il fatto costituisca reato:

a) l'organismo di valutazione della conformità che emette un certificato di cybersicurezza non conforme è punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. In caso di omessa revoca di un certificato da parte dell'organismo su richiesta dell'Agenzia, si applica la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro;

b) il fabbricante o fornitore che emette una dichiarazione UE di conformità volontaria non conforme è punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. In caso di omessa revisione o revoca di dichiarazione UE di conformità volontaria o obbligatoria ai sensi dell'articolo 7, comma 3, si applica la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro;

c) in caso di obbligatorietà di una dichiarazione UE di conformità o di un certificato di *cybersicurezza*, il fabbricante o fornitore che mette a disposizione sul mercato un prodotto TIC o servizio TIC privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza del certificato di cybersicurezza obbligatorio, è punito con la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato il fabbricante o fornitore che per la messa a disposizione sul mercato di un prodotto TIC o di un servizio TIC si avvale di un processo TIC privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza di certificato di *cybersicurezza* obbligatorio. Inoltre, l'Agenzia dispone il ritiro del prodotto o l'inibizione del servizio dal mercato a carico esclusivo del fabbricante o del fornitore indicando i tempi ed eventuali modalità per il richiamo dei prodotti già

[10] L'esercizio di tale potere sanzionatorio si pone in linea di coerenza con le previsioni di cui all'art. 7, comma 1, lett. e), del D.L. n. 82/2021, alla luce del quale l'Autorità nazionale di certificazione della *cybersicurezza* assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni.

immessi sul mercato o per l'inibizione del servizio. Il fornitore che non ottempera a quanto prescritto per l'inibizione del servizio dal mercato è assoggettato alla sanzione amministrativa da 60.000 euro a 300.000 euro;

d) il fabbricante che non ottempera a quanto prescritto per il richiamo di prodotti già immessi sul mercato è assoggettato alla sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. Nel caso in cui il fabbricante non ottemperi al richiamo di prodotti dal mercato, l'Agenzia, trascorsi sei mesi dalla scadenza fissata, può provvedere, al sequestro dei prodotti in questione dal mercato, a spese del fabbricante;

e) il titolare di un certificato europeo di *cybersicurezza* che non notifichi eventuali vulnerabilità o irregolarità rilevate in relazione alla sicurezza dei prodotti TIC, servizi TIC o processi TIC certificati è punito con la sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. Alla medesima sanzione è assoggettato l'organismo di valutazione della conformità emittente un certificato di *cybersicurezza* o il suo titolare ovvero il fornitore o fabbricante emittente una dichiarazione UE di conformità, che dovesse rilevare o venire a conoscenza della presenza di vulnerabilità nel prodotto TIC, servizio TIC o processo TIC certificato o dichiarato conforme, che non siano state riscontrate durante il processo di valutazione, e non ottemperi agli obblighi riguardanti il modo in cui segnalare e trattare le vulnerabilità previste per lo specifico sistema di certificazione;

f) il fabbricante o fornitore che non renda disponibile, per il periodo stabilito la dichiarazione UE di conformità o la documentazione tecnica o tutte le altre informazioni pertinenti o non trasmetta una copia della dichiarazione UE di conformità all'Agenzia o ad ENISA, ovvero non renda disponibili pubblicamente una o più delle informazioni previste ai sensi dell'art. 55 del Regolamento (UE) 2019/881[11] o non rispetti il formato o le procedure di aggiornamento delle stesse informazioni o pubblichi informazioni non corrette sui certificati detenuti o sulle dichiarazioni UE di

[11] Si riporta, per completezza l'art. 55 del Regolamento (UE) 2019/881:
Informazioni supplementari sulla cybersicurezza dei prodotti TIC, servizi TIC e processi TIC certificati
1. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC certificati o prodotti TIC, servizi TIC o processi per i quali è stata rilasciata una dichiarazione UE di conformità rende pubblicamente disponibili le seguenti informazioni supplementari sulla cybersicurezza:
a) orientamenti e raccomandazioni che assistano gli utenti finali nel configurare, installare, avviare, operare e mantenere in modo sicuro i prodotti TIC o servizi TIC;
b) il periodo durante il quale agli utenti finali sarà offerta assistenza di sicurezza, in particolare per quanto concerne la disponibilità di aggiornamenti connessi alla cybersicurezza;
c) informazioni di contatto del fabbricante o fornitore e metodi accettati per ricevere informazioni sulle vulnerabilità dagli utenti finali e dai ricercatori nel settore della sicurezza;
d) un riferimento ad archivi online in cui siano elencate le vulnerabilità comunicate al pubblico relative al prodotto TIC, servizio TIC o processo TIC e a tutti i relativi consigli in materia di cybersicurezza.
2. Le informazioni di cui al paragrafo 1 sono disponibili in formato elettronico, restano disponibili e sono aggiornate, ove necessario, almeno fino alla scadenza del certificato europeo di cybersicurezza o della dichiarazione UE di conformità corrispondenti.

conformità emesse, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato il fornitore o fabbricante che non comunichi la revisione o la revoca di una dichiarazione UE di conformità;

g) l'organismo di valutazione della conformità che non ottempera agli obblighi di divulgazione dei certificati europei di *cybersicurezza* rilasciati, modificati o revocati come previsto nell'ambito dello specifico sistema di certificazione è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato l'organismo di valutazione della conformità autorizzato dall'Agenzia che non specifichi nella procedura per i reclami l'inoltro degli stessi per conoscenza anche all'Agenzia;

h) nel caso di accertamento di esercizio di organismo di valutazione della conformità senza autorizzazione si applica la sanzione del pagamento di una somma da 120.000 euro a 600.000 euro e al soggetto non possono essere rilasciate ulteriori autorizzazioni nei successivi tre anni dall'accertamento della violazione. Se l'autorizzazione è scaduta da meno di un anno la sanzione è compresa tra 30.000 euro e 150.000 euro ed il soggetto può richiedere il rilascio di nuova autorizzazione;

i) il richiedente di una certificazione che nell'ambito dello svolgimento dell'attività di valutazione e di rilascio dei certificati, scientemente, fornisce dati, informazioni o documentazione falsi o ometta informazioni necessarie per espletare la certificazione è assoggettato alla sanzione del pagamento di una somma da 90.000 euro a 450.000 euro. Alla medesima sanzione è assoggettato il soggetto che, scientemente, durante le verifiche di vigilanza, a cui è sottoposto fornisce dati, informazioni o documentazione falsi;

l) il fabbricante che viola le condizioni di utilizzo degli eventuali marchi o etichette previste da un sistema europeo di certificazione è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro;

m) l'organismo di valutazione della conformità che non ottempera agli eventuali obblighi riguardanti la conservazione dei registri è assoggettato alla sanzione del pagamento di una somma da 45.000 euro a 225.000 euro.

Nel caso in cui, in esito ad un accertamento di non conformità, sia revocato o decada un certificato obbligatorio per la messa a disposizione sul mercato di un prodotto TIC o di un

servizio TIC, l'Agenzia dispone il ritiro del prodotto o l'inibizione del servizio dal mercato a carico esclusivo del fabbricante o del fornitore indicando i tempi ed eventuali modalità per il richiamo dei prodotti già immessi sul mercato o per l'inibizione del servizio; il fornitore che non ottempera a quanto prescritto per l'inibizione del servizio dal mercato è assoggettato alla sanzione amministrativa da 60.000 euro a 300.000 euro.

L'Agenzia, ai sensi del comma 15, dell'art. 10 del D.Lgs. n. 123/2022, può impartire ordini o intimare diffide ai soggetti che operano in contrasto con quanto previsto dal quadro europeo di certificazione. Ai soggetti che non ottemperano nel termine indicato nell'ordine o nella diffida l'Agenzia commina la sanzione del pagamento di una somma da 200.000 euro ad 1.000.000 di euro. Se le violazioni riguardano provvedimenti adottati dall'Agenzia nei confronti di soggetti con fatturato pari almeno a 200.000.000 euro[12], si applica a ciascun soggetto interessato una sanzione amministrativa pecuniaria non inferiore allo 0,3 per cento e non superiore all'1,5 per cento del fatturato, restando comunque fermo il limite massimo di 5.000.000 di euro.

I valori minimi e massimi di queste sanzioni pecuniarie sono triplicati, se la violazione ha riguardato un certificato relativo ad un prodotto TIC, ad un servizio TIC o ad un processo TIC rilasciato nell'ambito di un sistema di certificazione destinato all'utilizzo con le finalità o nell'ambito di un servizio essenziale o di un servizio di comunicazione elettronica. Resta, comunque fermo il limite di 5.000.000 di euro come sanzione massima applicabile.

Con un provvedimento dell'Agenzia (adottato secondo la procedura di cui all'art. 5, comma 3, del D.P.C.M. 9 dicembre 2021, n. 223) sono definiti i criteri di graduazione nell'irrogazione delle sanzioni pecuniarie[13].

L'autorizzazione di un organismo di valutazione della conformità ad operare nel sistema europeo di certificazione, ove prevista, è sospesa per 6 mesi o revocata nel caso di più di due violazioni del quadro europeo di certificazione rispettivamente in un quinquennio o in un biennio. In caso di revoca dell'autorizzazione, il trasgressore non può ottenere nuova autorizzazione nei successivi cinque anni dal provvedimento di revoca.

[12] Come riferimento per il fatturato si assume il valore realizzato dallo stesso soggetto nell'esercizio precedente a quello in cui sia stato impartito l'ordine o sia stata intimata la diffida.
[13] Nelle more dell'adozione del provvedimento in questione per la definizione dei criteri di graduazione si applicano i criteri di cui all'articolo 11 della legge 24 novembre 1981, n. 689, il quale dispone che *Nella determinazione della sanzione amministrativa pecuniaria fissata dalla legge tra un limite minimo ed un limite massimo e nell'applicazione delle sanzioni accessorie facoltative, si ha riguardo alla gravità della violazione, all'opera svolta dall'agente per la eliminazione o attenuazione delle conseguenze della violazione, nonché alla personalità dello stesso e alle sue condizioni economiche*.

9. I Reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità e il Ricorso all'autorità giudiziaria

Le persone fisiche e giuridiche, ai sensi dell'art. 11 del D.L. 123/2022, hanno il diritto di presentare un reclamo all'emittente di un certificato europeo di *cybersicurezza* o all'Agenzia se il reclamo riguarda un certificato europeo di *cybersicurezza* rilasciato dall'organismo di certificazione dell'Agenzia o da suo organismo di valutazione della conformità che agisce in conformità della normativa euro unitaria.

Avverso le decisioni degli organismi di valutazione della conformità diversi dall'organismo di certificazione può essere proposta procedura di reclamo a tal fine indicata dagli stessi organismi. Nel caso in cui i sistemi europei di certificazione della cybersicurezza stabiliscano requisiti specifici o supplementari per l'autorizzazione a svolgere i compiti da essi previsti, la procedura di reclamo indicata dall'organismo prevede l'inoltro del reclamo da parte del reclamante oltreché all'organismo anche per conoscenza all'Agenzia.

Avverso le decisioni dell'Agenzia riguardanti le certificazioni oppure le dichiarazioni UE di conformità rilasciate a seguito del processo di autovalutazione (ove consentito) i sensi dell'art. 53 del Regolamento (UE) 2019/881, può essere proposta procedura di reclamo. Il reclamante formula istanza all'Agenzia, identificando il certificato di *cybersicurezza* o la dichiarazione UE di conformità oggetto del reclamo, le ragioni del reclamo e le azioni correttive che ritiene necessarie.

L'Agenzia, a seguito tale tipologia di reclamo, informa il reclamante dello stato del procedimento e della decisione adottata e informa il reclamante del diritto a un ricorso giurisdizionale effettivo. L'Agenzia risponde ai reclami entro novanta giorni dal ricevimento dell'istanza. In caso di mancata risposta ad un reclamo inoltrato all'Agenzia entro i termini previsti, il reclamo si intende rigettato (c.d. *silenzio-rifiuto*).

Il successivo art. 12 riconosce a persone fisiche e giuridiche il diritto di impugnazione avverso:

a) le decisioni assunte dall'Agenzia o dagli organismi di valutazione della conformità, anche, se del caso, in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di *cybersicurezza* detenuto da tali persone fisiche e giuridiche;

b) il mancato o parziale accoglimento di un reclamo presentato all'Agenzia o agli organismi di valutazione della conformità.

9.1 Il Ricorso all'autorità giudiziaria

Il successivo art. 12 chiarisce che fatti salvi eventuali ricorsi amministrativi o altri ricorsi di tipo extragiudiziale, le persone fisiche e giuridiche possono proporre impugnazione avverso:

a) le decisioni assunte dall'Agenzia o dagli organismi di valutazione della conformità, anche, se del caso, in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di cybersicurezza detenuto da tali persone fisiche e giuridiche;

b) il mancato o parziale accoglimento di un reclamo presentato all'Agenzia o agli organismi di valutazione della conformità.

Il secondo comma del citato art. 12 chiarisce come tali impugnazioni siano devolute alla cognizione del giudice amministrativo. In particolare, i ricorsi contro le decisioni dell'Agenzia sono presentati dinanzi al tribunale amministrativo regionale del Lazio, mentre quelli contro le decisioni degli altri organismi di valutazione della conformità al tribunale amministrativo del luogo ove è ubicata la sede di tali organismi.

10. La Destinazione dei proventi derivanti dalle attività dell'Agenzia

Le attività di vigilanza, certificazione, autorizzazione, e abilitazione sono sottoposte a tariffa, da calcolarsi sulla base dei costi effettivi dei servizi resi[14] (art. 13, D.Lgs. n. 123/2022). Le tariffe e le modalità di riscossione sono determinate con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del Direttore generale dell'Agenzia. Tale decreto dispone, altresì, sulle modalità di calcolo delle spese per l'impiego di esperti o laboratori abilitati dall'Agenzia per le attività di vigilanza.

Gli introiti derivanti dalle sanzioni pecuniarie sono versati in un apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati con decreto del Ministro dell'economia e delle finanze sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione dei capitoli del bilancio

[14] I relativi proventi sono versati su di un apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati, con decreto del Ministro dell'economia e delle finanze, sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione degli appositi capitoli dell'Agenzia.

dell'Agenzia destinati alle attività di ricerca e formazione concernenti la certificazione della *cybersicurezza* di prodotti TIC, servizi TIC e processi TIC.

Le spese sostenute dall'Agenzia per l'adeguamento dei sistemi informativi sono coerenti con il *Piano triennale per l'informatica nella pubblica amministrazione* ai sensi dei commi da 512 a 520, dell'art. 1 della L. 28 dicembre 2015, n. 208 (art. 14).

Dall'attuazione del D.Lgs. n. 123/2022, ad esclusione dell'articolo 4, comma 3 (cfr. *supra*), non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e l'Agenzia provvede con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

Il Ministro dell'economia e delle finanze è autorizzato, dal quarto comma dell'art. 14, ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati.