2024/2847

20.11.2024

REGOLAMENTO (UE) 2024/2847 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 23 ottobre 2024

relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo [1],

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria [2],

considerando quanto segue:

(1) La cibersicurezza è una delle sfide principali per l'Unione. Il numero e la varietà dei dispositivi connessi aumenteranno esponenzialmente nei prossimi anni. Gli attacchi informatici costituiscono una questione di interesse pubblico dal momento che hanno un impatto determinante non solo sull'economia dell'Unione, ma anche sulla democrazia, nonché sulla sicurezza dei consumatori e sulla salute. Occorre pertanto rafforzare l'approccio dell'Unione alla cibersicurezza, occuparsi della ciberresilienza a livello dell'Unione nonché migliorare il funzionamento del mercato interno, definendo un quadro giuridico uniforme per i requisiti essenziali di cibersicurezza per l'immissione sul mercato dell'Unione di prodotti con elementi digitali. È opportuno affrontare i due problemi principali che comportano ulteriori costi per gli utilizzatori e la società: un basso livello di cibersicurezza dei prodotti con elementi digitali, testimoniato da vulnerabilità diffuse e dalla fornitura insufficiente e incoerente di aggiornamenti di sicurezza per porvi rimedio così come un'insufficiente comprensione delle informazioni e un accesso limitato alle stesse da parte degli utilizzatori, che impediscono loro di scegliere prodotti con proprietà di cibersicurezza adeguate o di utilizzarli in modo sicuro.

(2) Il presente regolamento mira a stabilire le condizioni limite per lo sviluppo di prodotti con elementi digitali sicuri, garantendo che i prodotti hardware e software siano immessi sul mercato con un minor numero di vulnerabilità e che i fabbricanti prendano la sicurezza in seria considerazione durante l'intero ciclo di vita di un prodotto. Si propone inoltre di creare le condizioni che consentano agli utilizzatori di tenere conto della cibersicurezza nella scelta e nell'utilizzo dei prodotti con elementi digitali, ad esempio migliorando la trasparenza per quanto riguarda il periodo di assistenza dei prodotti con elementi digitali messi a disposizione sul mercato.

(3) Il pertinente diritto dell'Unione in vigore comprende diverse serie di norme orizzontali che affrontano taluni aspetti legati alla cibersicurezza da diversi punti di vista, comprese misure per migliorare la sicurezza della catena di approvvigionamento digitale. Tuttavia il diritto dell'Unione vigente in materia di cibersicurezza, tra cui il regolamento (UE) 2019/881 del Parlamento e del Consiglio [3] e la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio [4], non contempla direttamente requisiti obbligatori per la sicurezza dei prodotti con elementi digitali.

---

[1] GU C 100 del 16.3.2023, pag. 101.

[2] Posizione del Parlamento europeo del 12 marzo 2024 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 10 ottobre 2024.

[3] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (GU L 151 del 7.6.2019, pag. 15).

[4] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80).

(4) Sebbene il diritto dell'Unione vigente si applichi a determinati prodotti con elementi digitali, non esiste un quadro normativo orizzontale dell'Unione che stabilisca requisiti di cibersicurezza completi per tutti i prodotti con elementi digitali. I vari atti adottati e le diverse iniziative intraprese finora a livello nazionale e dell'Unione affrontano solo parzialmente i problemi e i rischi individuati in materia di cibersicurezza, creando un mosaico legislativo all'interno del mercato interno, aumentando l'incertezza del diritto sia per i fabbricanti sia per gli utilizzatori di tali prodotti e imponendo alle imprese e alle organizzazioni un onere aggiuntivo inutile per conformarsi a una serie di requisiti e obblighi per tipi di prodotti simili. La cibersicurezza di tali prodotti ha una dimensione transfrontaliera particolarmente forte, poiché i prodotti con elementi digitali fabbricati in uno Stato membro o in un paese terzo sono spesso utilizzati da organizzazioni e consumatori in tutto il mercato interno. Ciò rende necessaria una regolamentazione del settore a livello dell'Unione per garantire un quadro normativo armonizzato e la certezza del diritto per gli utilizzatori, le organizzazioni e le imprese, comprese le microimprese e le piccole e medie imprese quali definite nell'allegato della raccomandazione 2003/361/CE della Commissione ([5]). Il panorama normativo dell'Unione dovrebbe essere armonizzato introducendo requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali. Inoltre si dovrebbe garantire la certezza del diritto per gli operatori economici e gli utilizzatori in tutta l'Unione, nonché una migliore armonizzazione del mercato interno e proporzionalità per le micro, piccole e medie imprese, creando condizioni più agevoli per gli operatori economici che intendono entrare in tale mercato.

(5) Per quanto riguarda le microimprese e le piccole e medie imprese, nel determinare la categoria in cui rientra un'impresa dovrebbero essere applicate integralmente le disposizioni dell'allegato della raccomandazione 2003/361/CE. Pertanto, nel calcolo degli effettivi e delle soglie finanziarie che definiscono le categorie di imprese, dovrebbero essere applicate anche le disposizioni dell'articolo 6 dell'allegato della raccomandazione 2003/361/CE relativa alla determinazione dei dati di un'impresa in considerazione di tipi specifici di imprese, quali imprese associate o collegate.

(6) La Commissione dovrebbe fornire orientamenti per assistere gli operatori economici, in particolare le microimprese e le piccole e medie imprese, nell'applicazione del presente regolamento. Tali orientamenti dovrebbero riguardare, tra l'altro, l'ambito di applicazione del presente regolamento, in particolare il trattamento dei dati a distanza e le sue implicazioni per gli sviluppatori di software liberi e open source, l'applicazione dei criteri utilizzati per determinare i periodi di assistenza per i prodotti con elementi digitali, l'interazione tra il presente regolamento e altre disposizioni di diritto dell'Unione e il concetto di modifica sostanziale.

(7) A livello dell'Unione diversi documenti programmatici e politici, come la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 16 dicembre 2020, dal titolo «La strategia dell'UE in materia di cibersicurezza per il decennio digitale», le conclusioni del Consiglio del 2 dicembre 2020 sulla cibersicurezza dei dispositivi connessi e del 23 maggio 2022 sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica e la risoluzione del Parlamento europeo del 10 giugno 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale ([6]), hanno chiesto l'introduzione di requisiti specifici dell'Unione in materia di cibersicurezza per i prodotti digitali o connessi e diversi paesi terzi hanno adottato di propria iniziativa misure volte ad affrontare la questione. Nella relazione finale della Conferenza sul futuro dell'Europa, i cittadini hanno chiesto «un ruolo più incisivo dell'UE nella lotta contro le minacce alla cibersicurezza». Affinché l'Unione possa svolgere un ruolo di primo piano a livello internazionale nel settore della cibersicurezza, è importante istituire un quadro normativo ambizioso.

(8) Per aumentare il livello generale di cibersicurezza di tutti i prodotti con elementi digitali immessi sul mercato interno è necessario introdurre requisiti essenziali di cibersicurezza orientati agli obiettivi e tecnologicamente neutri per tali prodotti, applicabili orizzontalmente.

(9) In determinate condizioni tutti i prodotti con elementi digitali integrati in un sistema di informazione elettronico più ampio o connessi a un tale sistema possono fungere da vettore di attacco per soggetti malintenzionati. Di conseguenza anche l'hardware e il software che sono considerati meno critici possono facilitare la compromissione iniziale di un dispositivo o di una rete, consentendo a soggetti malintenzionati di ottenere un accesso privilegiato a un sistema o di muoversi lateralmente tra sistemi. I fabbricanti dovrebbero pertanto garantire che tutti i prodotti con elementi digitali siano progettati e sviluppati conformemente ai requisiti essenziali di cibersicurezza stabiliti nel presente regolamento. Tale obbligo si riferisce sia ai prodotti che possono essere connessi in modo fisico tramite interfacce hardware sia ai prodotti che sono connessi in modo logico, ad esempio tramite *socket* di rete, pipe, file, interfacce per programmi applicativi o qualsiasi altro tipo di interfaccia software. Poiché le minacce informatiche possono propagarsi attraverso vari prodotti con elementi digitali prima di raggiungere un determinato obiettivo, ad esempio concatenando più exploit di vulnerabilità, i fabbricanti dovrebbero garantire la cibersicurezza anche dei prodotti con elementi digitali che sono connessi solo indirettamente ad altri dispositivi o reti.

([5]) Raccomandazione della Commissione 2003/361/CE, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

([6]) GU C 67 dell'8.2.2022, pag. 81.

(10) Stabilendo requisiti di cibersicurezza per l'immissione sul mercato di prodotti con elementi digitali, si intende migliorare la cibersicurezza di tali prodotti sia per i consumatori che per le imprese. Tali requisiti garantiranno inoltre che la cibersicurezza sia presa in considerazione in tutte le catene di approvvigionamento, rendendo più sicuri i prodotti finali con elementi digitali e i loro componenti. Ciò include anche requisiti per l'immissione sul mercato di prodotti di consumo con elementi digitali destinati ai consumatori vulnerabili, come giocattoli e sistemi di monitoraggio dei neonati. I prodotti di consumo con elementi digitali classificati nel presente regolamento come prodotti con elementi digitali importanti presentano un rischio di cibersicurezza più elevato in quanto svolgono una funzione che comporta un rischio significativo di effetti negativi in termini di intensità e capacità di danneggiare la salute, la sicurezza o l'incolumità degli utilizzatori di tali prodotti e dovrebbero essere sottoposti a una procedura di valutazione della conformità più rigorosa. Ciò vale per prodotti quali i prodotti per case intelligenti con funzionalità di sicurezza, comprese serrature intelligenti, sistemi di monitoraggio dei neonati e sistemi di allarme, giocattoli connessi e tecnologie sanitarie indossabili personali. Inoltre, le procedure di valutazione della conformità più rigorose cui devono essere sottoposti altri prodotti con elementi digitali classificati nel presente regolamento come prodotti con elementi digitali importanti o critici contribuiranno a prevenire gli effetti negativi che lo sfruttamento delle vulnerabilità può avere sui consumatori.

(11) L'obiettivo del presente regolamento è garantire un livello elevato di cibersicurezza dei prodotti con elementi digitali e delle loro soluzioni integrate di elaborazione dati da remoto. Tali soluzioni di elaborazione dati da remoto dovrebbero essere definite come una elaborazione dati a distanza per la quale il software è stato progettato e sviluppato dal fabbricante del prodotto con elementi digitali in questione o per suo conto, la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni. Tale approccio garantisce che tali prodotti siano protetti adeguatamente nella loro interezza dai fabbricanti, indipendentemente dal fatto che i dati siano trattati o conservati localmente sul dispositivo dell'utente o a distanza dal fabbricante. Allo stesso tempo, il trattamento o l'archiviazione a distanza rientrano nell'ambito di applicazione del presente regolamento solo nella misura in cui sono necessari affinché un prodotto con elementi digitali svolga le sue funzioni. Tale trattamento o archiviazione a distanza comprende l'eventualità in cui un'applicazione mobile richieda l'accesso a un'interfaccia per programmi applicativi o a una banca dati fornita tramite un servizio sviluppato dal fabbricante. In tal caso, il servizio rientra nell'ambito di applicazione del presente regolamento come soluzione di elaborazione dati da remoto. I requisiti relativi alle soluzioni di elaborazione dati da remoto che rientrano nell'ambito di applicazione del presente regolamento non comportano pertanto misure tecniche, operative o organizzative volte a gestire i rischi posti alla sicurezza dei sistemi informativi e di rete di un fabbricante nel loro complesso.

(12) Le soluzioni cloud costituiscono soluzioni di elaborazione dati da remoto ai sensi del presente regolamento solo se soddisfano la definizione di cui al presente regolamento. Ad esempio, le funzionalità abilitate al cloud fornite da un fabbricante di dispositivi per case intelligenti che consentono agli utilizzatori di controllare il dispositivo a distanza rientrano nell'ambito di applicazione del presente regolamento. D'altro canto, i siti web che non supportano la funzionalità di un prodotto con elementi digitali o i servizi cloud la cui progettazione e il cui sviluppo esulano dalla responsabilità del fabbricante di un prodotto con elementi digitali non rientrano nell'ambito di applicazione del presente regolamento. La direttiva (UE) 2022/2555 si applica ai servizi di cloud computing e ai modelli di servizi cloud quali il servizio a livello di software (*Software-as-a-Service* – SaaS), il servizio a livello di piattaforma (*Platform-as-a-Service* – PaaS) o il servizio a livello di infrastruttura *(Infrastructure-as-a-Service* – IaaS). I soggetti che forniscono servizi di cloud computing nell'Unione che si qualificano come medie imprese ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE, o che superano le soglie per le medie imprese di cui al paragrafo 1 di detto articolo, rientrano nell'ambito di applicazione di tale direttiva.

(13) Conformemente all'obiettivo del presente regolamento di rimuovere gli ostacoli alla libera circolazione dei prodotti con elementi digitali, gli Stati membri non dovrebbero impedire, per gli aspetti disciplinati dal presente regolamento, la messa a disposizione sul mercato di prodotti con elementi digitali che sono conformi al presente regolamento. Pertanto, per le questioni armonizzate dal presente regolamento, gli Stati membri non possono imporre requisiti di cibersicurezza supplementari per la messa a disposizione sul mercato di prodotti con elementi digitali. Qualsiasi soggetto, pubblico o privato, può tuttavia stabilire requisiti supplementari rispetto a quelli stabiliti nel presente regolamento per l'acquisto o l'uso di prodotti con elementi digitali per sue finalità specifiche e può pertanto scegliere di utilizzare prodotti con elementi digitali che soddisfano requisiti di cibersicurezza più rigorosi o più specifici di quelli applicabili alla messa a disposizione sul mercato a norma del presente regolamento. Fatte salve le direttive 2014/24/UE ([7]) e 2014/25/UE ([8]) del Parlamento europeo e del Consiglio, nell'acquistare prodotti con elementi digitali che devono essere conformi ai requisiti essenziali di cibersicurezza di cui al presente regolamento, compresi quelli relativi alla gestione delle vulnerabilità, gli Stati membri dovrebbero garantire che tali requisiti siano presi in

([7]) Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

([8]) Direttiva 2014/25/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali e che abroga la direttiva 2004/17/CE (GU L 94 del 28.3.2014, pag. 243).

considerazione nella procedura di appalto e che si tenga conto anche della capacità dei fabbricanti di applicare efficacemente misure di cibersicurezza e di gestire le minacce informatiche. Inoltre, la direttiva (UE) 2022/2555 stabilisce misure di gestione dei rischi di cibersicurezza per i soggetti essenziali e importanti di cui all'articolo 3 di detta direttiva. Tali misure potrebbero comportare misure di sicurezza della catena di approvvigionamento che richiedono l'uso da parte di detti soggetti di prodotti con elementi digitali che soddisfino requisiti di cibersicurezza più rigorosi di quelli stabiliti nel presente regolamento. Conformemente alla direttiva (UE) 2022/2555 e in linea con il suo principio di armonizzazione minima, gli Stati membri possono pertanto imporre requisiti di cibersicurezza supplementari per l'uso di prodotti delle tecnologie dell'informazione e della comunicazione (TIC) da parte di soggetti essenziali o importanti ai sensi di tale direttiva al fine di garantire un livello più elevato di cibersicurezza, a condizione che tali requisiti siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione. Le questioni non disciplinate dal presente regolamento possono includere fattori non tecnici riguardanti i prodotti con elementi digitali e i relativi fabbricanti. Gli Stati membri possono pertanto stabilire misure nazionali, comprese restrizioni sui prodotti con elementi digitali o sui fornitori di tali prodotti, che tengano conto di fattori non tecnici. Le misure nazionali relative a tali fattori devono essere conformi al diritto dell'Unione.

(14) Il presente regolamento non dovrebbe pregiudicare la responsabilità degli Stati membri di tutelare la sicurezza nazionale, nel rispetto del diritto dell'Unione. Gli Stati membri dovrebbero poter sottoporre i prodotti con elementi digitali acquistati o utilizzati a fini di sicurezza nazionale o di difesa a misure supplementari, a condizione che tali misure siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione.

(15) Il presente regolamento si applica agli operatori economici solo in relazione ai prodotti con elementi digitali messi a disposizione sul mercato, quindi ai prodotti forniti per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale. La fornitura nel corso di un'attività commerciale può essere caratterizzata non solo dall'applicazione di un prezzo per un prodotto con elementi digitali, ma anche dall'applicazione di un prezzo per i servizi di assistenza tecnica quando ciò non è finalizzato esclusivamente a recuperare i costi effettivi, dall'intenzione di monetizzare, ad esempio dalla fornitura di una piattaforma software attraverso la quale il fabbricante monetizza altri servizi, dall'imposizione, come condizione per l'utilizzo, del trattamento di dati personali per motivi diversi dal solo miglioramento della sicurezza, della compatibilità o dell'interoperabilità del software, o dall'accettazione di donazioni che superano i costi associati alla progettazione, allo sviluppo e alla fornitura di un prodotto con elementi digitali. L'atto di accettare donazioni senza fini di lucro non dovrebbe essere considerato costitutivo di un'attività commerciale.

(16) I prodotti con elementi digitali forniti nell'ambito della prestazione di un servizio per il quale è addebitata una tariffa esclusivamente per recuperare i costi effettivi direttamente connessi alla gestione di tale servizio, come nel caso di determinati prodotti con elementi digitali forniti da enti della pubblica amministrazione, non dovrebbero essere considerati costitutivi di un'attività commerciale ai fini del presente regolamento solamente per tali motivi. Inoltre, i prodotti con elementi digitali sviluppati o modificati da un ente della pubblica amministrazione esclusivamente per uso proprio non dovrebbero essere considerati quali prodotti messi a disposizione sul mercato ai sensi del presente regolamento.

(17) I software e i dati che sono condivisi apertamente e che gli utilizzatori possono liberamente consultare, utilizzare, modificare e ridistribuire, comprese le loro versioni modificate, possono contribuire alla ricerca e all'innovazione nel mercato. Per promuovere lo sviluppo e l'utilizzo di software liberi e open source, in particolare da parte delle microimprese e delle piccole e medie imprese, tra cui le start-up, degli individui, delle organizzazioni senza scopo di lucro e degli istituti di ricerca accademica, l'applicazione del presente regolamento ai prodotti con elementi digitali che si qualificano come software liberi e open source forniti per la distribuzione o l'utilizzo nel corso di un'attività commerciale dovrebbe tenere conto della natura dei diversi modelli di sviluppo di software che sono distribuiti e sviluppati con licenze software libere e open source.

(18) Per software libero e open source si intende un software il cui codice sorgente è condiviso apertamente e la cui concessione di licenze prevede tutti i diritti affinché sia liberamente accessibile, utilizzabile, modificabile e ridistribuibile. Il software libero e open source è sviluppato, sottoposto a manutenzione e distribuito apertamente, anche tramite piattaforme online. Per quanto riguarda gli operatori economici che rientrano nell'ambito di applicazione del presente regolamento, solo i software liberi e open source messi a disposizione sul mercato e pertanto forniti per essere distribuiti o utilizzati nel corso di un'attività commerciale dovrebbero rientrare nell'ambito di applicazione del presente regolamento. Le mere circostanze in cui il prodotto con elementi digitali è stato sviluppato o il modo in cui lo sviluppo è stato finanziato non dovrebbero pertanto essere presi in considerazione al fine di determinare la natura commerciale o non commerciale di tale attività. Più specificamente, ai fini del presente regolamento e in relazione agli operatori economici che rientrano nel suo ambito di applicazione, per garantire che tra la fase di sviluppo e la fase di fornitura vi sia una chiara distinzione, la fornitura di prodotti con

elementi digitali che si qualificano come software liberi e open source che non sono monetizzati dai loro fabbricanti non dovrebbe essere considerata un'attività commerciale. Inoltre, la fornitura di prodotti con elementi digitali che si qualificano come componenti software liberi e open source destinati a essere integrati da altri fabbricanti nei rispettivi prodotti con elementi digitali dovrebbe essere considerata come messa a disposizione sul mercato solo se il componente è monetizzato dal suo fabbricante originario. Ad esempio, il semplice fatto che un prodotto software open source con elementi digitali riceva sostegno finanziario dai fabbricanti o che questi ultimi contribuiscano allo sviluppo di tale prodotto non dovrebbe di per sé determinare che un'attività sia di carattere commerciale. Inoltre, il semplice fatto che siano rilasciate con cadenza regolare nuove versioni non dovrebbe di per sé far concludere che un prodotto con elementi digitali è fornito nel corso di un'attività commerciale. Infine, ai fini del presente regolamento, lo sviluppo di prodotti con elementi digitali che si qualificano come di software liberi e open source da parte di organizzazioni senza scopo di lucro non dovrebbe essere considerato costitutivo di un'attività commerciale, a condizione che l'organizzazione sia costituita in modo tale da garantire che tutti gli utili al netto dei costi siano utilizzati per conseguire obiettivi senza scopo di lucro. Il presente regolamento non si applica alle persone fisiche o giuridiche che contribuiscono tramite codici sorgente a prodotti con elementi digitali che si qualificano come software liberi e open source che esulano dalla loro responsabilità.

19) Tenendo conto dell'importanza per la cibersicurezza di molti prodotti con elementi digitali che si qualificano come software liberi e open source che sono pubblicati ma non messi a disposizione sul mercato ai sensi del presente regolamento, le persone giuridiche che forniscono un sostegno duraturo per lo sviluppo di tali prodotti destinati ad attività commerciali e che svolgono un ruolo fondamentale nel garantire la sostenibilità economica di tali prodotti (gestori di software open source) dovrebbero essere soggette a un regime normativo semplificato e su misura. Sono gestori di software open source anche determinate fondazioni e soggetti che sviluppano e pubblicano software liberi e open source in un contesto commerciale, compresi i soggetti senza scopo di lucro. Il regime normativo dovrebbe tener conto della loro natura specifica e della loro compatibilità con il tipo di obblighi imposti. Dovrebbe riguardare solo i prodotti con elementi digitali che si qualificano come software liberi e open source destinati in ultima istanza ad attività commerciali, ad esempio quelli destinati all'integrazione in servizi commerciali o in prodotti monetizzati con elementi digitali. Ai fini di tale regime normativo, l'intento di integrazione in prodotti monetizzati con elementi digitali riguarda anche i casi in cui i fabbricanti che integrano un componente nei propri prodotti con elementi digitali contribuiscono con regolarità allo sviluppo di tale componente o forniscono regolarmente assistenza finanziaria per garantire la continuità di un prodotto software. Apportare un sostegno duraturo allo sviluppo di un prodotto con elementi digitali comprende, tra l'altro, l'hosting e la gestione di piattaforme di collaborazione per lo sviluppo di software, l'hosting di codici sorgente o software, l'amministrazione o la gestione di prodotti con elementi digitali che si qualificano come software liberi e open source, nonché l'orientamento dello sviluppo di tali prodotti. Dato che tale regime normativo semplificato e su misura non assoggetta coloro che fungono da gestori di software open source agli stessi obblighi di coloro che fungono da fabbricanti a norma del presente regolamento, detti gestori non dovrebbero essere autorizzati ad apporre la marcatura CE sui prodotti con elementi digitali di cui sostengono lo sviluppo.

(20) Il solo fatto di ospitare prodotti con elementi digitali in archivi aperti, anche tramite gestori di pacchetti o su piattaforme di collaborazione, non costituisce di per sé una messa a disposizione sul mercato di un prodotto con elementi digitali. I fornitori di tali servizi dovrebbero essere considerati distributori solo se mettono tale software a disposizione sul mercato e quindi se lo forniscono per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale.

(21) Al fine di sostenere e agevolare la dovuta diligenza dei fabbricanti che integrano componenti software liberi e open source non soggetti ai requisiti essenziali di cibersicurezza di cui al presente regolamento nei loro prodotti con elementi digitali, la Commissione dovrebbe poter istituire programmi volontari di attestazione di sicurezza, o mediante un atto delegato che integra il presente regolamento o richiedendo un sistema europeo di certificazione della cibersicurezza a norma dell'articolo 48 del regolamento (UE) 2019/881 che tenga conto delle specificità dei modelli di sviluppo di software liberi e open source. I programmi di attestazione di sicurezza dovrebbero essere concepiti in modo tale che non solo le persone fisiche o giuridiche che sviluppano o contribuiscono allo sviluppo di un prodotto con elementi digitali che si qualificano come software liberi e open source possano avviare o finanziare un'attestazione di sicurezza, ma che lo possano fare anche terzi, come i fabbricanti che integrano tali prodotti nei propri prodotti con elementi digitali, gli utilizzatori o le pubbliche amministrazioni dell'Unione e nazionali.

(22) Alla luce degli obiettivi pubblici di cibersicurezza del presente regolamento e al fine di migliorare la conoscenza situazionale degli Stati membri per quanto riguarda la dipendenza dell'Unione dai componenti software e, in particolare, dai componenti software potenzialmente liberi e open source, un apposito gruppo di cooperazione amministrativa (ADCO) istituito dal presente regolamento dovrebbe poter decidere di effettuare congiuntamente una valutazione della dipendenza dell'Unione. Le autorità di vigilanza del mercato dovrebbero poter chiedere ai fabbricanti di categorie di prodotti con elementi digitali stabilite dall'ADCO di presentare le distinte base del software che hanno generato a norma del presente regolamento. Al fine di tutelare la riservatezza delle distinte base del software, le autorità di vigilanza del mercato dovrebbero trasmettere all'ADCO le informazioni pertinenti sulle dipendenze in forma anonimizzata e aggregata.

(23) L'efficacia dell'attuazione del presente regolamento dipenderà anche dalla disponibilità di competenze adeguate in materia di cibersicurezza. A livello dell'Unione, vari documenti programmatici e politici, tra cui la comunicazione della Commissione, del 18 aprile 2023, dal titolo «Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE» e le conclusioni del Consiglio, del 22 maggio 2023, sulla politica di ciberdifesa dell'UE hanno riconosciuto il divario di competenze in materia di cibersicurezza nell'Unione e la necessità di affrontare tali sfide in via prioritaria, sia nel settore pubblico che in quello privato. Al fine di garantire un'efficace attuazione del presente regolamento, gli Stati membri dovrebbero assicurare che le autorità di vigilanza del mercato e gli organismi di valutazione della conformità abbiano a loro disponibilità risorse adeguate per poter impiegare il personale necessario allo svolgimento dei loro compiti, come stabilito nel presente regolamento. Tali misure dovrebbero migliorare la mobilità della forza lavoro nel settore della cibersicurezza e i relativi percorsi professionali. Dovrebbero inoltre contribuire a rendere la forza lavoro nel settore della cibersicurezza più resiliente e inclusiva, anche in termini di genere. Gli Stati membri dovrebbero pertanto adottare misure per garantire che tali compiti siano svolti da professionisti adeguatamente formati, dotati delle necessarie competenze in materia di cibersicurezza. Analogamente, i fabbricanti dovrebbero garantire che il loro personale disponga delle competenze necessarie per adempiere agli obblighi stabiliti dal presente regolamento. Gli Stati membri e la Commissione, in linea con le rispettive prerogative e competenze e con i compiti specifici loro attribuiti dal presente regolamento, dovrebbero adottare misure per sostenere i fabbricanti, in particolare le microimprese e le piccole e medie imprese, comprese le start-up, anche in settori quali lo sviluppo delle competenze, ai fini del rispetto dei loro obblighi quali stabiliti nel presente regolamento. Inoltre, poiché la direttiva (UE) 2022/2555 impone agli Stati membri, nell'ambito delle loro strategie nazionali relative alla cibersicurezza, di adottare politiche volte a promuovere e sviluppare la formazione nella cibersicurezza e competenze in materia di cibersicurezza, gli Stati membri, nell'adottare tali strategie, possono inoltre prendere in considerazione di affrontare il fabbisogno di competenze in materia di cibersicurezza derivante dal presente regolamento, compreso quello relativo alla riqualificazione e al miglioramento delle competenze.

(24) Lo sviluppo di un'Internet sicura è indispensabile per il funzionamento delle infrastrutture critiche e per la società nel suo complesso. La direttiva (UE) 2022/2555 mira a garantire un livello elevato di cibersicurezza dei servizi forniti dai soggetti essenziali e importanti di cui all'articolo 3 di tale direttiva, compresi i fornitori di infrastrutture digitali che sostengono le funzioni fondamentali dell'Internet aperta e garantiscono i servizi Internet e forniscono l'accesso a Internet. È quindi importante che i prodotti con elementi digitali necessari ai fornitori di infrastrutture digitali per garantire il funzionamento di Internet siano sviluppati in modo sicuro e siano conformi a norme di sicurezza Internet consolidate. Il presente regolamento, che si applica a tutti i prodotti hardware e software collegabili, mira anche a facilitare il rispetto dei requisiti relativi alla catena di approvvigionamento a norma della direttiva (UE) 2022/2555 da parte dei fornitori di infrastrutture digitali, garantendo che i prodotti con elementi digitali che essi utilizzano per la fornitura dei loro servizi siano sviluppati in modo sicuro e che abbiano accesso ad aggiornamenti di sicurezza tempestivi per tali prodotti.

(25) Il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio ([9]) stabilisce norme relative ai dispositivi medici e il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ([10]) stabilisce norme relative ai dispositivi medico-diagnostici in vitro. Tali regolamenti si occupano di rischi di cibersicurezza e adottano approcci specifici che sono trattati anche nel presente regolamento. Più in particolare i regolamenti (UE) 2017/745 e (UE) 2017/746 stabiliscono i requisiti essenziali per i dispositivi medici che funzionano attraverso un sistema elettronico o che sono essi stessi software. Tali regolamenti disciplinano anche alcuni software non incorporati e l'approccio dell'intero ciclo di vita. Tali requisiti impongono ai fabbricanti di sviluppare e costruire i loro prodotti applicando principi di gestione del rischio e definendo requisiti relativi alle misure di sicurezza informatica, nonché corrispondenti procedure di valutazione della conformità. Inoltre da dicembre 2019 sono in vigore orientamenti specifici sulla cibersicurezza per i dispositivi medici, che forniscono ai fabbricanti di dispositivi medici, inclusi i dispositivi diagnostici in vitro, indicazioni su come soddisfare tutti i requisiti essenziali pertinenti di cui all'allegato I di tali regolamenti per quanto riguarda la cibersicurezza. I prodotti con elementi digitali a cui si applica uno dei due regolamenti non dovrebbero pertanto essere soggetti al presente regolamento.

(26) I prodotti con elementi digitali sviluppati o modificati esclusivamente per scopi di sicurezza nazionale o di difesa o i prodotti specificamente progettati per trattare informazioni classificate non rientrano nell'ambito di applicazione del presente regolamento. Gli Stati membri sono incoraggiati a garantire per tali prodotti un livello di protezione uguale o superiore a quello dei prodotti che rientrano nell'ambito di applicazione del presente regolamento.

([9]) Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

([10]) Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

(27) Il regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio ([11]) stabilisce i requisiti per l'omologazione dei veicoli e dei loro sistemi e componenti, introducendo taluni requisiti di cibersicurezza riguardanti, tra l'altro, il funzionamento di un sistema certificato di gestione della cibersicurezza e gli aggiornamenti del software, disciplinando le politiche e i processi delle organizzazioni per i rischi di cibersicurezza relativi all'intero ciclo di vita dei veicoli, dei dispositivi e dei servizi in conformità dei regolamenti delle Nazioni Unite applicabili in materia di specifiche tecniche e cibersicurezza, in particolare il regolamento n. 155 delle Nazioni Unite – Disposizioni uniformi relative all'omologazione dei veicoli per quanto riguarda la cibersicurezza e i sistemi di gestione della cibersicurezza ([12]), e prevedendo specifiche procedure di valutazione della conformità. Nel settore dell'aviazione, il regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio ([13]) ha come obiettivo principale stabilire e mantenere un livello elevato ed uniforme di sicurezza dell'aviazione civile nell'Unione. Esso istituisce un quadro di requisiti essenziali per l'aeronavigabilità di prodotti aeronautici, parti ed equipaggiamenti, compreso il software, che comprendono gli obblighi di protezione dalle minacce alla security delle informazioni. Il processo di certificazione a norma del regolamento (UE) 2018/1139 assicura il livello di garanzia perseguito dal presente regolamento. I prodotti con elementi digitali a cui si applica il regolamento (UE) 2019/2144 e i prodotti certificati in conformità del regolamento (UE) 2018/1139 non dovrebbero pertanto soggetti ai requisiti essenziali di cibersicurezza e alle procedure di valutazione della conformità di cui al presente regolamento.

(28) Il presente regolamento stabilisce norme orizzontali in materia di cibersicurezza che non sono specifiche per settori o per determinati prodotti con elementi digitali. Tuttavia potrebbero essere introdotte norme dell'Unione settoriali o specifiche per prodotto, volte a stabilire requisiti che affrontano tutti o alcuni dei rischi contemplati dai requisiti essenziali di cibersicurezza stabiliti nel presente regolamento. In tali casi l'applicazione del presente regolamento ai prodotti con elementi digitali contemplati da altre norme dell'Unione, che stabiliscono requisiti che affrontano tutti o alcuni dei rischi contemplati dai requisiti essenziali di cibersicurezza di cui al presente regolamento, può essere limitata o esclusa, qualora tale limitazione o esclusione sia coerente con il quadro normativo generale applicabile a tali prodotti e qualora le norme settoriali conseguano almeno lo stesso livello di protezione previsto dal presente regolamento. È opportuno conferire alla Commissione il potere di adottare atti delegati per integrare il presente regolamento individuando tali prodotti e norme. Per quanto riguarda il diritto dell'Unione vigente in cui dovrebbe essere applicata tale limitazione o esclusione, il presente regolamento prevede disposizioni specifiche per chiarire il suo rapporto con tale diritto dell'Unione.

(29) Al fine di garantire che i prodotti con elementi digitali messi a disposizione sul mercato possano essere riparati in modo efficace e che la loro durabilità possa essere estesa, è opportuno prevedere un'esenzione per i pezzi di ricambio. Tale esenzione dovrebbe riguardare sia i pezzi di ricambio che hanno lo scopo di riparare prodotti preesistenti messi a disposizione prima della data di applicazione del presente regolamento sia i pezzi di ricambio che sono già stati sottoposti a una procedura di valutazione della conformità ai sensi del presente regolamento.

(30) Il regolamento delegato (UE) 2022/30 della Commissione ([14]) specifica che alcuni dei requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) e f), della direttiva 2014/53/UE del Parlamento europeo e del Consiglio ([15]), relativi ai danni alla rete e abuso delle risorse della rete, ai dati personali e vita privata e alle frodi, si applicano a determinate apparecchiature radio. La decisione di esecuzione C(2022)5637 della Commissione, del 5 agosto 2022, relativa ad una richiesta di normazione rivolta al Comitato europeo di normazione e al Comitato europeo di normazione elettrotecnica stabilisce i requisiti per l'elaborazione di norme specifiche, precisando inoltre il modo in cui dovrebbero essere trattati tali requisiti essenziali. I requisiti essenziali di cibersicurezza stabiliti dal presente regolamento comprendono tutti gli elementi dei requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) e f),

([11]) Regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n. 79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti della Commissione (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010, (UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011, (UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012, (UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 (GU L 325 del 16.12.2019, pag. 1).

([12]) GU L 82 del 9.3.2021, pag. 30.

([13]) Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1).

([14]) Regolamento delegato (UE) 2022/30 della Commissione, del 29 ottobre 2021, che integra la direttiva 2014/53/UE del Parlamento europeo e del Consiglio per quanto riguarda l'applicazione dei requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) ed f), di tale direttiva (GU L 7 del 12.1.2022, pag. 6).

([15]) Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (GU L 153 del 22.5.2014, pag. 62).

della direttiva 2014/53/UE. I requisiti essenziali di cibersicurezza stabiliti nel presente regolamento sono inoltre allineati con gli obiettivi dei requisiti delle norme specifiche incluse in tale richiesta di normazione. Pertanto, quando la Commissione abroga o modifica il regolamento delegato (UE) 2022/30, con la conseguenza che esso cessa di applicarsi a determinati prodotti soggetti al presente regolamento, la Commissione e le organizzazioni europee di normazione dovrebbero tenere conto dei lavori di normazione svolti nel contesto della decisione di esecuzione C (2022)5637 nella preparazione e nello sviluppo di norme armonizzate per facilitare l'attuazione del presente regolamento. Durante il periodo di transizione per l'applicazione del presente regolamento, la Commissione dovrebbe fornire orientamenti ai fabbricanti soggetti al presente regolamento che sono anche soggetti al regolamento delegato (UE) 2022/30, al fine di agevolare la dimostrazione della conformità ai due regolamenti.

(31) La direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio ([16]) è complementare al presente regolamento. Tale direttiva stabilisce le norme in materia di responsabilità per danno da prodotti difettosi, in modo che i danneggiati possano chiedere il risarcimento quando un danno è stato causato da prodotti difettosi. Essa stabilisce il principio secondo cui il fabbricante di un prodotto è responsabile dei danni causati da una mancanza di sicurezza nel suo prodotto indipendentemente dalla colpa (responsabilità oggettiva). Se tale mancanza di sicurezza consiste nell'assenza di aggiornamenti di sicurezza dopo l'immissione sul mercato del prodotto e ciò causa un danno, questo potrebbe far scattare la responsabilità del fabbricante. Gli obblighi dei fabbricanti relativi alla fornitura di tali aggiornamenti di sicurezza dovrebbero essere stabiliti nel presente regolamento.

(32) Il presente regolamento dovrebbe lasciare impregiudicato il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([17]), comprese le disposizioni relative all'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità a detto regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Tali operazioni potrebbero essere integrate in un prodotto con elementi digitali. La protezione dei dati fin dalla progettazione e per impostazione predefinita e la cibersicurezza in generale sono elementi fondamentali del regolamento (UE) 2016/679. Proteggendo i consumatori e le organizzazioni dai rischi di cibersicurezza, i requisiti essenziali di cibersicurezza stabiliti nel presente regolamento dovrebbero inoltre contribuire a migliorare la protezione dei dati personali e della vita privata delle persone. Dovrebbero essere considerate le sinergie sia nell'ambito della normazione che della certificazione relativamente agli aspetti di cibersicurezza attraverso la cooperazione tra la Commissione, le organizzazioni europee di normazione, l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), il comitato europeo per la protezione dei dati istituito dal regolamento (UE) 2016/679 e le autorità nazionali di controllo della protezione dei dati. È opportuno creare sinergie tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati anche nel settore della vigilanza del mercato e dell'applicazione delle norme. A tal fine le autorità nazionali di vigilanza del mercato designate a norma del presente regolamento dovrebbero cooperare con le autorità preposte alla vigilanza dell'applicazione del diritto dell'Unione in materia di protezione dei dati. Queste ultime dovrebbero inoltre avere accesso alle informazioni pertinenti per lo svolgimento dei loro compiti.

(33) Nella misura in cui i loro prodotti rientrano nell'ambito di applicazione del presente regolamento, i fornitori dei portafogli europei di identità digitale di cui all'articolo 5 *bis*, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([18]) dovrebbero essere conformi sia ai requisiti essenziali orizzontali di cibersicurezza stabiliti dal presente regolamento sia ai requisiti di sicurezza specifici stabiliti dall'articolo 5 *bis* del regolamento (UE) n. 910/2014. Al fine di facilitare la conformità, i fornitori dei portafogli dovrebbero poter dimostrare la conformità dei portafogli europei di identità digitale ai requisiti stabiliti rispettivamente nel presente regolamento e nel regolamento (UE) n. 910/2014 certificando i loro prodotti nell'ambito di un sistema europeo di certificazione della cibersicurezza istituito a norma del regolamento (UE) 2019/881 e per il quale la Commissione ha specificato, mediante atti delegati, una presunzione di conformità al presente regolamento, nella misura in cui il certificato o sue parti contemplino tali requisiti.

(34) Quando integrano componenti provenienti da terzi in prodotti con elementi digitali durante la fase di progettazione e sviluppo, i fabbricanti dovrebbero, al fine di garantire che i prodotti siano progettati, sviluppati e fabbricati conformemente ai requisiti essenziali di cibersicurezza di cui al presente regolamento, esercitare la dovuta diligenza per quanto riguarda tali componenti, compresi i componenti software liberi e open source che non sono stati messi

([16]) Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio(GU L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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) (GU L 119 del 4.5.2016, pag. 1).

([18]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

a disposizione sul mercato. Il livello adeguato di dovuta diligenza dipende dalla natura e dal livello di rischio di cibersicurezza associato a un dato componente e a tal fine dovrebbe tenere conto di una o più delle seguenti azioni: verifica, se del caso, che il fabbricante di un componente abbia dimostrato la conformità al presente regolamento, anche controllando che il componente rechi già la marcatura CE; verifica che un componente riceva aggiornamenti periodici di sicurezza, ad esempio controllando i precedenti aggiornamenti di sicurezza; verifica che un componente sia privo di vulnerabilità registrate nella banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555 o in altre banche dati delle vulnerabilità accessibili al pubblico; oppure svolgimento di ulteriori prove di sicurezza. Gli obblighi di gestione delle vulnerabilità di cui al presente regolamento, che i fabbricanti devono rispettare quando immettono sul mercato un prodotto con elementi digitali e durante il periodo di assistenza, si applicano ai prodotti con elementi digitali nella loro interezza, compresi tutti i componenti integrati. Qualora, nell'esercizio della dovuta diligenza, il fabbricante del prodotto con elementi digitali individui una vulnerabilità in un componente, anche in un componente libero e open source, dovrebbe informare la persona o il soggetto che si occupa della fabbricazione o della manutenzione del componente, affrontare e correggere la vulnerabilità e, se del caso, fornire alla persona o al soggetto la correzione di sicurezza applicata.

(35) Immediatamente dopo il periodo di transizione per l'applicazione del presente regolamento, un fabbricante di un prodotto con elementi digitali che integra uno o più componenti provenienti da terzi che sono anche soggetti al presente regolamento potrebbe non essere in grado di verificare, nell'ambito del suo obbligo di dovuta diligenza, che i fabbricanti di tali componenti abbiano dimostrato la conformità al presente regolamento controllando, ad esempio, se i componenti recano già la marcatura CE. Ciò può verificarsi quando i componenti sono stati integrati prima che il presente regolamento sia diventato applicabile ai fabbricanti di tali componenti. In tal caso, il fabbricante che integra tali componenti dovrebbe esercitare la dovuta diligenza con altri mezzi.

(36) I prodotti con elementi digitali dovrebbero recare la marcatura CE per indicare in modo visibile, leggibile e indelebile la loro conformità al presente regolamento, in modo da poter circolare liberamente nel mercato interno. Gli Stati membri non dovrebbero ostacolare in maniera ingiustificata l'immissione sul mercato di prodotti con elementi digitali che soddisfano i requisiti stabiliti nel presente regolamento e che recano la marcatura CE. Inoltre, in occasione di fiere, mostre e dimostrazioni o eventi analoghi, gli Stati membri non dovrebbero impedire la presentazione o l'uso di un prodotto con elementi digitali non conforme al presente regolamento, compresi i suoi prototipi, a condizione che il prodotto presenti un'indicazione visibile che specifichi chiaramente che esso non è conforme al presente regolamento e non deve essere messo a disposizione sul mercato finché non lo sarà.

(37) Per far sì che i fabbricanti possano rilasciare software ai fini di prova prima di sottoporre i loro prodotti con elementi digitali alla valutazione della conformità, gli Stati membri non dovrebbero impedire la messa a disposizione di software non finiti, come versioni alfa, versioni beta o release candidate, a condizione che il software non finito sia messo a disposizione solo per il tempo necessario a testarlo e a raccogliere riscontri. I fabbricanti dovrebbero provvedere affinché il software messo a disposizione a tali condizioni sia rilasciato solo a seguito di una valutazione dei rischi e sia conforme, per quanto possibile, ai requisiti di sicurezza relativi alle proprietà dei prodotti con elementi digitali stabiliti dal presente regolamento. I fabbricanti dovrebbero inoltre attuare, nella misura del possibile, i requisiti di gestione delle vulnerabilità. I fabbricanti non dovrebbero costringere gli utilizzatori a passare alle versioni rilasciate solo ai fini di prova.

(38) Per garantire che i prodotti con elementi digitali, quando sono immessi sul mercato, non presentino rischi di cibersicurezza per le persone e le organizzazioni, è opportuno stabilire requisiti essenziali di cibersicurezza per tali prodotti. Tali requisiti essenziali di cibersicurezza, compresi i requisiti in materia di gestione delle vulnerabilità, si applicano a ogni singolo prodotto con elementi digitali al momento dell'immissione sul mercato, indipendentemente dal fatto che il prodotto con elementi digitali sia fabbricato come unità singola o in serie. Ad esempio, per un tipo di prodotto, ogni singolo prodotto con elementi digitali dovrebbe aver ricevuto tutte le patch o gli aggiornamenti di sicurezza disponibili per affrontare le questioni di sicurezza pertinenti al momento dell'immissione sul mercato. Qualora i prodotti con elementi digitali vengano successivamente modificati, da mezzi fisici o digitali, in un modo non previsto dal fabbricante nella valutazione dei rischi iniziale e che potrebbe implicare il fatto che essi non rispettino più i requisiti essenziali di cibersicurezza pertinenti, la modifica dovrebbe essere considerata sostanziale. Ad esempio le riparazioni potrebbero essere assimilate a interventi di manutenzione purché non modifichino un prodotto con elementi digitali già immesso sul mercato in maniera tale da poter influire sulla sua conformità ai requisiti applicabili o da modificare la finalità prevista per la quale il prodotto è stato valutato.

(39) Come avviene per le modifiche o le riparazioni fisiche, un prodotto con elementi digitali dovrebbe essere considerato modificato sostanzialmente da un cambiamento del software qualora l'aggiornamento del software modifichi la finalità prevista di tale prodotto e tali modifiche non siano state previste dal fabbricante nella valutazione dei rischi iniziale, o qualora la natura del pericolo sia cambiata o il livello di rischio di cibersicurezza sia aumentato a causa

dell'aggiornamento del software e la versione aggiornata del prodotto sia messa a disposizione sul mercato. Qualora non modifichi la finalità prevista di un prodotto con elementi digitali, un aggiornamento di sicurezza, progettato per ridurre il livello di rischio di cibersicurezza di un prodotto con elementi digitali, non è considerato una modifica sostanziale. Sono generalmente inclusi i casi in cui un aggiornamento di sicurezza comporta solo adeguamenti minori del codice sorgente. Ad esempio, tale caso potrebbe verificarsi quando un aggiornamento di sicurezza affronta una vulnerabilità nota, anche modificando le funzioni o le prestazioni di un prodotto con elementi digitali al solo scopo di ridurre il livello di rischio di cibersicurezza. Analogamente, un aggiornamento minore delle funzionalità, come ad esempio un miglioramento visivo, o l'aggiunta di nuovi pittogrammi o lingue all'interfaccia utente, non dovrebbe, di norma, essere considerato una modifica sostanziale. Per contro, qualora modifichi le funzioni originariamente previste o il tipo o le prestazioni di un prodotto con elementi digitali e soddisfi tali criteri, un aggiornamento delle funzioni dovrebbe essere considerato una modifica sostanziale, in quanto l'aggiunta di nuove caratteristiche determina di norma una superficie di attacco più ampia, con un conseguente aumento del rischio di cibersicurezza. Ad esempio, tale caso potrebbe verificarsi quando un nuovo elemento di input viene aggiunto a un'applicazione, il che impone al fabbricante di garantire un'adeguata convalida dell'input. Nel valutare se un aggiornamento delle funzioni sia considerato una modifica sostanziale non è rilevante che sia fornito come aggiornamento separato o in combinazione con un aggiornamento di sicurezza. La Commissione dovrebbe emanare orientamenti sulle modalità per determinare il concetto di «modifica sostanziale».

(40) Tenuto conto del carattere iterativo dello sviluppo di software, i fabbricanti che hanno immesso sul mercato versioni successive di un prodotto software a seguito di una successiva modifica sostanziale di tale prodotto dovrebbero poter fornire aggiornamenti di sicurezza per il periodo di assistenza solo per l'ultima versione del prodotto software che hanno immesso sul mercato. Dovrebbero poter farlo solo se gli utilizzatori delle pertinenti versioni precedenti del prodotto hanno accesso all'ultima versione del prodotto immessa sul mercato gratuitamente e non sostengono costi aggiuntivi per adeguare l'ambiente hardware o software in cui funziona il prodotto. Tale caso potrebbe verificarsi, ad esempio, quando un aggiornamento del sistema operativo desktop non richiede un nuovo hardware, come un'unità centrale di elaborazione più veloce o più memoria. Tuttavia, il fabbricante dovrebbe continuare a rispettare, per il periodo di assistenza, altri requisiti di gestione delle vulnerabilità, ad esempio dotandosi di una politica in materia di divulgazione coordinata delle vulnerabilità o predisponendo misure volte ad agevolare la condivisione di informazioni sulle potenziali vulnerabilità per tutte le successive versioni del prodotto software immesso sul mercato che sono state modificate in modo sostanziale. I fabbricanti dovrebbero poter fornire aggiornamenti minori di sicurezza o delle funzionalità che non costituiscono una modifica sostanziale solo per l'ultima versione o sottoversione di un prodotto software che non è stato modificato in modo sostanziale. Nel contempo, qualora un prodotto hardware, come uno smartphone, non sia compatibile con l'ultima versione del sistema operativo con cui è stato originariamente fornito, il fabbricante dovrebbe continuare a fornire aggiornamenti di sicurezza almeno per l'ultima versione compatibile del sistema operativo per il periodo di assistenza.

(41) In linea con il concetto generalmente riconosciuto di modifica sostanziale dei prodotti disciplinati dalla normativa di armonizzazione dell'Unione, qualora intervenga una modifica sostanziale che può incidere sulla conformità di un prodotto con elementi digitali al presente regolamento oppure quando venga modificata la sua finalità prevista, è opportuno verificare la conformità del prodotto con elementi digitali e sottoporlo, se del caso, a una nuova valutazione della conformità. Ove applicabile, se il fabbricante effettua una valutazione della conformità che coinvolge terzi, i cambiamenti che potrebbero comportare una modifica sostanziale dovrebbero essere notificati a questi ultimi.

(42) Se un prodotto con elementi digitali è soggetto a «ricondizionamento», «manutenzione» e «riparazione», quali definiti all'articolo 2, punti 18), 19) e 20), del regolamento (UE) 2024/2781 del Parlamento europeo e del Consiglio ([19]), ciò non comporta necessariamente una modifica sostanziale del prodotto, ad esempio se la finalità e le funzionalità previste non sono modificate e il livello di rischio rimane inalterato. Tuttavia il miglioramento di un prodotto con elementi digitali da parte del fabbricante potrebbe comportare modifiche nella progettazione e nello sviluppo del prodotto stesso e quindi influire sulla sua finalità prevista e sulla sua conformità ai requisiti stabiliti nel presente regolamento.

(43) I prodotti con elementi digitali dovrebbero essere considerati importanti se lo sfruttamento di potenziali vulnerabilità di cibersicurezza nel prodotto può provocare un impatto negativo grave a causa, tra l'altro, della funzionalità legata alla cibersicurezza o di una funzione che comporta un rischio significativo di avere effetti negativi in termini della sua intensità e capacità di perturbare, controllare o danneggiare un gran numero di altri prodotti con elementi digitali o la salute, la sicurezza o l'incolumità dei suoi utilizzatori attraverso la manipolazione diretta, come una funzione centrale di sistema centrale, compresi la gestione della rete, il controllo di configurazione, la virtualizzazione o il trattamento dei dati personali. In particolare le vulnerabilità nei prodotti con elementi digitali dotati di una funzionalità legata alla cibersicurezza, come i boot manager, possono determinare una propagazione dei problemi di sicurezza lungo l'intera catena di approvvigionamento. La gravità dell'impatto di un incidente può

([19]) Regolamento (UE) 2024/1781 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce il quadro per la definizione dei requisiti di progettazione ecocompatibile per prodotti sostenibili, modifica la direttiva (UE) 2020/1828 e il regolamento (UE) 2023/1542 e abroga la direttiva 2009/125/CE(GU L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

anche aumentare se il prodotto svolge principalmente una funzione di sistema centrale, tra cui la gestione della rete, il controllo di configurazione, la virtualizzazione o il trattamento di dati personali.

(44) Talune categorie di prodotti con elementi digitali dovrebbero essere soggetti a procedure di valutazione della conformità più rigorose, pur mantenendo un approccio proporzionato. A tal fine i prodotti con elementi digitali importanti dovrebbero essere suddivisi in due classi che riflettono il livello di rischio di cibersicurezza legato a tali categorie di prodotti. Un incidente che coinvolga prodotti con elementi digitali importanti di classe II potrebbe avere impatti negativi maggiori rispetto a un incidente che coinvolga prodotti con elementi digitali importanti di classe I, ad esempio a causa della natura della loro funzione legata alla cibersicurezza o dello svolgimento di un'altra funzione che comporta un rischio significativo di effetti negativi. Come indicazione di tali impatti negativi maggiori, i prodotti con elementi digitali di classe II potrebbero svolgere una funzionalità legata alla cibersicurezza o un'altra funzione che comporta un rischio significativo di effetti negativi più elevato rispetto a quelli elencati nella classe I, o soddisfare entrambi i criteri summenzionati. I prodotti con elementi digitali importanti di classe II dovrebbero pertanto essere soggetti a una procedura di valutazione della conformità più rigorosa.

(45) I prodotti con elementi digitali importanti di cui al presente regolamento dovrebbero essere intesi come prodotti che hanno la funzionalità principale di una categoria di prodotti con elementi digitali importanti stabilita nel presente regolamento. Il presente regolamento stabilisce ad esempio categorie di prodotti con elementi digitali importanti che, in base alla loro funzionalità principale, sono definiti firewall o sistemi di rilevamento o prevenzione delle intrusioni di classe II. Di conseguenza i firewall o i sistemi di rilevamento o prevenzione delle intrusioni sono soggetti a una valutazione della conformità obbligatoria da parte di terzi. Ciò non si applica ad altri prodotti con elementi digitali non categorizzati come prodotti con elementi digitali importanti che possono integrare firewall o sistemi di rilevamento o prevenzione delle intrusioni. La Commissione dovrebbe adottare un atto di esecuzione per precisare la descrizione tecnica delle categorie di prodotti con elementi digitali importanti rientranti nelle classi I e II di cui al presente regolamento.

(46) Le categorie di prodotti con elementi digitali critici di cui al presente regolamento hanno una funzionalità legata alla cibersicurezza e svolgono una funzione che comporta un rischio significativo di effetti negativi in termini di intensità e capacità di perturbare, controllare o recare danno a un gran numero di altri prodotti con elementi digitali mediante manipolazione diretta. Inoltre, tali categorie di prodotti con elementi digitali sono considerate dipendenze critiche dei soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555. Le categorie di prodotti con elementi digitali critici stabiliti in allegato al presente regolamento, a causa della loro criticità, utilizzano già ampiamente varie forme di certificazione e rientrano anche nel sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) di cui al regolamento di esecuzione (UE) 2024/482 della Commissione ([20]). Pertanto, al fine di garantire una protezione comune adeguata della cibersicurezza dei prodotti con elementi digitali critici nell'Unione, potrebbe essere opportuno e proporzionato assoggettare tali categorie di prodotti, mediante un atto delegato, a una certificazione europea obbligatoria della cibersicurezza qualora sia già in vigore un pertinente sistema europeo di certificazione della cibersicurezza riguardante tali prodotti e la Commissione abbia effettuato una valutazione del potenziale impatto sul mercato della certificazione obbligatoria prevista. Tale valutazione dovrebbe valutare sia il lato dell'offerta che quello della domanda, compresa l'esistenza di una domanda sufficiente dei prodotti con elementi digitali interessati sia da parte degli Stati membri che degli utilizzatori per richiedere la certificazione europea della cibersicurezza, nonché le finalità per le quali i prodotti con elementi digitali sono destinati a essere utilizzati, compresa la dipendenza critica da essi dei soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555. La valutazione dovrebbe inoltre analizzare i potenziali effetti della certificazione obbligatoria sulla disponibilità di tali prodotti sul mercato interno e le capacità e la prontezza degli Stati membri per l'attuazione dei pertinenti sistemi europei di certificazione della cibersicurezza.

(47) Gli atti delegati che richiedono una certificazione europea obbligatoria della cibersicurezza dovrebbero determinare i prodotti con elementi digitali che hanno la funzionalità principale di una categoria di prodotti con elementi digitali critici di cui al presente regolamento che devono essere soggetti a certificazione obbligatoria, nonché il livello di garanzia richiesto, che dovrebbe essere almeno «sostanziale». Il livello di garanzia richiesto dovrebbe essere proporzionato al livello di rischio di cibersicurezza associato al prodotto con elementi digitali. Ad esempio, se il prodotto con elementi digitali ha la funzionalità principale di una categoria di prodotti con elementi digitali critici di

([20]) Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) (GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

cui al presente regolamento ed è destinato all'uso in un ambiente sensibile o critico, come i prodotti destinati all'uso dei soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555, esso può richiedere il livello di garanzia più elevato.

(48) Al fine di garantire una protezione comune adeguata della cibersicurezza nell'Unione per i prodotti con elementi digitali che hanno la funzionalità principale di una categoria di prodotti con elementi digitali critici di cui al presente regolamento, alla Commissione dovrebbe inoltre essere conferito il potere di adottare atti delegati per modificare il presente regolamento aggiungendo ulteriori categorie di prodotti con elementi digitali critici per le quali i fabbricanti potrebbero essere tenuti a ottenere un certificato europeo di cibersicurezza nell'ambito di un sistema europeo di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881 per dimostrare la conformità al presente regolamento o ritirando categorie esistenti. Una nuova categoria di prodotti con elementi digitali critici può essere aggiunta a tali categorie se sussiste una dipendenza critica da essi da parte dei soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555 oppure se, in caso di incidenti o di vulnerabilità sfruttate, ciò potrebbe causare perturbazioni delle catene di approvvigionamento critiche. Nel valutare la necessità di aggiungere o ritirare categorie di prodotti con elementi digitali critici mediante un atto delegato, la Commissione dovrebbe poter considerare se gli Stati membri abbiano individuato a livello nazionale prodotti con elementi digitali che svolgono un ruolo critico per la resilienza dei soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555 e che affrontano in misura crescente attacchi informatici alla catena di approvvigionamento, con potenziali gravi effetti perturbatori. Inoltre, la Commissione dovrebbe poter tenere conto dell'esito della valutazione coordinata a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche effettuata a norma dell'articolo 22 della direttiva (UE) 2022/2555.

(49) La Commissione dovrebbe garantire che nell'elaborazione delle misure per l'attuazione del presente regolamento sia consultato un ampio ventaglio di pertinenti portatori di interessi in modo strutturato e regolare. Ciò dovrebbe valere in particolare quando la Commissione valuta la necessità di potenziali aggiornamenti degli elenchi delle categorie di prodotti con elementi digitali importanti o critici, caso in cui i pertinenti fabbricanti dovrebbero essere consultati e i loro pareri dovrebbero essere presi in considerazione al fine di analizzare i rischi di cibersicurezza e l'equilibrio tra costi e benefici della designazione di tali categorie di prodotti come importanti o critici.

(50) Il presente regolamento affronta i rischi di cibersicurezza in modo mirato. I prodotti con elementi digitali possono tuttavia comportare altri rischi di sicurezza che non sono sempre connessi alla cibersicurezza ma che possono essere la conseguenza di una violazione della sicurezza. Tali rischi dovrebbero continuare a essere regolamentati da altre normative di armonizzazione dell'Unione pertinenti diverse dal presente regolamento. Se non sono applicabili altre normative di armonizzazione dell'Unione diverse dal presente regolamento, essi dovrebbero essere soggetti al regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio ([21]).Pertanto, alla luce della natura mirata del presente regolamento, in deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento (UE) 2023/988, il capo III, sezione 1, i capi V e VII e i capi da IX a XI del regolamento (UE) 2023/988 dovrebbero applicarsi ai prodotti con elementi digitali per quanto riguarda i rischi di sicurezza non contemplati dal presente regolamento, qualora tali prodotti non siano soggetti a requisiti specifici stabiliti da altre normative di armonizzazione dell'Unione diverse dal presente regolamento ai sensi dell'articolo 3, punto 27), del regolamento (UE) 2023/988.

(51) I prodotti con elementi digitali classificati come sistemi di IA ad alto rischio a norma dell'articolo 6 del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio ([22]) che rientrano nell'ambito di applicazione del presente regolamento dovrebbero essere conformi ai requisiti essenziali di cibersicurezza stabiliti da quest'ultimo. Se soddisfano i requisiti essenziali di cibersicurezza stabiliti nel presente regolamento, tali sistemi di IA ad alto rischio dovrebbero essere considerati conformi ai requisiti di cibersicurezza stabiliti all'articolo 15 del regolamento (UE) 2024/1689 nella misura in cui tali requisiti siano contemplati dalla dichiarazione di conformità UE, o da sue parti, rilasciata a norma del presente regolamento. A tal fine la valutazione dei rischi di cibersicurezza associati a un prodotto con elementi digitali classificato come sistema di IA ad alto rischio a norma del regolamento (UE) 2024/1689 di cui si deve tenere conto durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto, come previsto dal presente regolamento, dovrebbe considerare i rischi alla ciberresilienza di un sistema di IA per quanto riguarda i tentativi di terzi non autorizzati di alterarne l'uso, il

([21]) Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio, del 10 maggio 2023, relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE (GU L 135 del 23.5.2023, pag. 1).

([22]) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

comportamento o le prestazioni, comprese le vulnerabilità specifiche dell'IA come l'avvelenamento dei dati o gli attacchi antagonistici, così come, se del caso, i rischi ai diritti fondamentali conformemente al regolamento (UE) 2024/1689. Per quanto riguarda le procedure di valutazione della conformità relative ai requisiti essenziali di cibersicurezza di un prodotto con elementi digitali che rientra nell'ambito di applicazione del presente regolamento e che è classificato come sistema di IA ad alto rischio, è opportuno che si applichi come norma generale l'articolo 43 del regolamento (UE) 2024/1689 anziché le pertinenti disposizioni del presente regolamento. Tuttavia tale norma non dovrebbe comportare una riduzione del livello di garanzia necessario per i prodotti con elementi digitali importanti o critici di cui al presente regolamento. Pertanto, in deroga a tale norma, i sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del regolamento (UE) 2024/1689 e che sono anche prodotti con elementi digitali importanti o critici di cui al presente regolamento e ai quali si applica la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI del regolamento (UE) 2024/1689 dovrebbero essere soggetti alle procedure di valutazione della conformità di cui al presente regolamento per quanto riguarda i requisiti essenziali di cibersicurezza stabiliti nello stesso. In tal caso, per tutti gli altri aspetti contemplati dal regolamento (UE) 2024/1689, è opportuno applicare le pertinenti disposizioni in materia di valutazione della conformità basata sul controllo interno di cui all'allegato VI di tale regolamento.

(52) Per migliorare la sicurezza dei prodotti con elementi digitali immessi sul mercato interno occorre stabilire requisiti essenziali di cibersicurezza applicabili a tali prodotti. Tali requisiti essenziali di cibersicurezza non dovrebbero pregiudicare le valutazioni dei rischi di sicurezza coordinate a livello dell'Unione delle catene di approvvigionamento critiche di cui all'articolo 22 della direttiva (UE) 2022/2555, che tengono conto sia dei fattori di rischio tecnici sia, se pertinente, di quelli non tecnici, come l'indebita influenza di un paese terzo sui fornitori. Inoltre non dovrebbero pregiudicare la prerogativa degli Stati membri di stabilire requisiti aggiuntivi che tengano conto di fattori non tecnici al fine di garantire un livello elevato di resilienza, compresi quelli definiti nella raccomandazione (UE) 2019/534 della Commissione ([23]), nella valutazione dei rischi coordinata dell'UE della cibersicurezza delle reti 5G e nel pacchetto di strumenti dell'UE sulla cibersicurezza del 5G concordato dal gruppo di cooperazione istituito a norma dell'articolo 14 della direttiva (UE) 2022/2555.

(53) I fabbricanti di prodotti che rientrano nell'ambito di applicazione del regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio ([24]) che sono anche prodotti con elementi digitali come definiti nel presente regolamento dovrebbero rispettare sia i requisiti essenziali di cui al presente regolamento sia i requisiti essenziali di cibersicurezza di cui al presente regolamento e di tutela della salute di cui al regolamento (UE) 2023/1230. I requisiti essenziali di cibersicurezza di cui al presente regolamento e alcuni requisiti essenziali stabiliti nel regolamento (UE) 2023/1230 potrebbero affrontare rischi di cibersicurezza simili. La conformità ai requisiti essenziali di cibersicurezza di cui al presente regolamento potrebbe pertanto facilitare la conformità ai requisiti essenziali che coprono anche determinati rischi di cibersicurezza di cui al regolamento (UE) 2023/1230, in particolare quelli riguardanti la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo di cui all'allegato III, sezioni 1.1.9 e 1.2.1, di tale regolamento. Tali sinergie devono essere dimostrate dal fabbricante, ad esempio attraverso l'applicazione, se disponibili, di norme armonizzate o altre specifiche tecniche riguardanti i requisiti essenziali di cibersicurezza pertinenti a seguito di una valutazione dei rischi che copra tali rischi di cibersicurezza. Il fabbricante dovrebbe inoltre seguire le procedure di valutazione della conformità applicabili di cui al presente regolamento e al regolamento (UE) 2023/1230. La Commissione e le organizzazioni europee di normazione, nei lavori preparatori a sostegno dell'attuazione del presente regolamento e del regolamento (UE) 2023/1230 e dei relativi processi di normazione, dovrebbero promuovere la coerenza nel modo in cui sono valutati i rischi di cibersicurezza e nel modo in cui tali rischi devono essere contemplati da norme armonizzate per quanto riguarda i requisiti essenziali pertinenti. In particolare, la Commissione e le organizzazioni europee di normazione dovrebbero tenere conto del presente regolamento nella preparazione e nello sviluppo di norme armonizzate per agevolare l'attuazione del regolamento (UE) 2023/1230 per quanto concerne, in particolare, gli aspetti di cibersicurezza relativi alla protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo di cui all'allegato III, sezioni 1.1.9 e 1.2.1, di tale regolamento. La Commissione dovrebbe fornire orientamenti per sostenere i fabbricanti soggetti al presente regolamento che sono anche soggetti al regolamento (UE) 2023/1230, in particolare per facilitare la dimostrazione della conformità ai pertinenti requisiti essenziali di cui al presente regolamento e al regolamento (UE) 2023/1230.

(54) Al fine di garantire che i prodotti con elementi digitali siano sicuri sia al momento dell'immissione sul mercato sia durante il periodo in cui si prevede di utilizzare il prodotto con elementi digitali, è necessario stabilire requisiti essenziali di cibersicurezza per la gestione delle vulnerabilità e requisiti essenziali di cibersicurezza relativi alle proprietà dei prodotti con elementi digitali. Se da un lato i fabbricanti dovrebbero soddisfare tutti i requisiti

([23]) Raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, Cibersicurezza delle reti 5G (GU L 88 del 29.3.2019, pag. 42).

([24]) Regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio, del 14 giugno 2023, relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio (GU L 165 del 29.6.2023, pag. 1).

essenziali di cibersicurezza relativi alla gestione delle vulnerabilità per tutto il periodo di assistenza, dall'altro dovrebbero determinare quali altri requisiti essenziali relativi alle proprietà del prodotto sono pertinenti per il tipo di prodotto con elementi digitali in questione. A tal fine è opportuno che i fabbricanti effettuino una valutazione dei rischi di cibersicurezza associati a un prodotto con elementi digitali per identificare i rischi e i requisiti essenziali di cibersicurezza pertinenti per rendere disponibili i loro prodotti con elementi digitali senza vulnerabilità note sfruttabili che possano avere un impatto sulla sicurezza di tali prodotti e per applicare in modo appropriato le norme armonizzate, le specifiche comuni o le norme europee o internazionali adeguate.

(55) Se alcuni requisiti essenziali di cibersicurezza non sono applicabili a un prodotto con elementi digitali, il fabbricante dovrebbe fornire una chiara giustificazione nella valutazione dei rischi di cibersicurezza inclusa nella documentazione tecnica. Ciò potrebbe verificarsi quando un requisito essenziale di cibersicurezza è incompatibile con la natura di un prodotto con elementi digitali. Ad esempio, la finalità prevista di un prodotto con elementi digitali può imporre al fabbricante di seguire norme di interoperabilità ampiamente riconosciute anche se le relative caratteristiche di sicurezza non sono più considerate all'avanguardia. Analogamente, altre disposizioni di diritto dell'Unione impongono ai fabbricanti di applicare specifici requisiti in materia di interoperabilità. Qualora un requisito essenziale di cibersicurezza non sia applicabile a un prodotto con elementi digitali ma il fabbricante abbia individuato rischi di cibersicurezza in relazione a tale requisito essenziale di cibersicurezza, dovrebbe adottare misure per affrontare tali rischi con altri mezzi, ad esempio limitando la finalità prevista del prodotto ad ambienti sicuri o informando gli utilizzatori di tali rischi.

(56) Una delle misure più importanti che gli utilizzatori possono adottare per proteggere i loro prodotti con elementi digitali da attacchi informatici consiste nell'installare quanto prima gli ultimi aggiornamenti di sicurezza disponibili. I fabbricanti dovrebbero pertanto progettare i prodotti e mettere in atto processi per far sì che i prodotti con elementi digitali includano funzioni che consentano la notifica, la distribuzione, il download e l'installazione di aggiornamenti di sicurezza in modo automatico, specie nel caso dei prodotti di consumo. Dovrebbero inoltre prevedere la possibilità di approvare il download e l'installazione degli aggiornamenti di sicurezza come ultimo passaggio. Agli utilizzatori dovrebbe essere garantita la possibilità di disattivare gli aggiornamenti automatici attraverso un sistema chiaro e di facile utilizzo, supportato da istruzioni chiare sulla procedura di disattivazione. I requisiti relativi agli aggiornamenti automatici di cui all'allegato del presente regolamento non si applicano ai prodotti con elementi digitali destinati principalmente a essere integrati come componenti in altri prodotti. Esse non si applicano neppure ai prodotti con elementi digitali per i quali gli utilizzatori non si attenderebbero ragionevolmente aggiornamenti automatici, compresi i prodotti con elementi digitali destinati a essere utilizzati nelle reti TIC professionali, e in particolare in ambienti critici e industriali in cui un aggiornamento automatico potrebbe interferire con le operazioni. Indipendentemente dal fatto che un prodotto con elementi digitali sia progettato o meno per ricevere aggiornamenti automatici, il fabbricante dovrebbe informare gli utilizzatori in merito alle vulnerabilità e rendere disponibili senza indugio gli aggiornamenti di sicurezza. Se un prodotto con elementi digitali dispone di un'interfaccia utente o di mezzi tecnici analoghi che consentono un'interazione diretta con i suoi utilizzatori, il fabbricante dovrebbe utilizzare tali funzionalità per informare gli utilizzatori che il suo prodotto con elementi digitali ha raggiunto la fine del periodo di assistenza. Le notifiche dovrebbero limitarsi a quanto necessario per garantire l'effettiva ricezione di tali informazioni e non dovrebbero avere un impatto negativo sull'esperienza di chi utilizza il prodotto con elementi digitali.

(57) Per migliorare la trasparenza dei processi di gestione delle vulnerabilità e garantire che gli utilizzatori non siano tenuti a installare nuovi aggiornamenti di funzionalità al solo scopo di ricevere gli ultimi aggiornamenti di sicurezza, i fabbricanti dovrebbero garantire, ove tecnicamente fattibile, che i nuovi aggiornamenti di sicurezza siano forniti separatamente dagli aggiornamenti di funzionalità.

(58) La comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 20 giugno 2023, dal titolo «Strategia europea per la sicurezza economica» ha affermato che l'Unione deve massimizzare i benefici della sua apertura economica, riducendo al contempo il più possibile i rischi derivanti dalla dipendenza economica da fornitori ad alto rischio, attraverso un quadro strategico comune per la sicurezza economica dell'Unione. La dipendenza da fornitori ad alto rischio di prodotti con elementi digitali può comportare un rischio strategico che deve essere affrontato a livello dell'Unione, in particolare quando i prodotti con elementi digitali sono destinati a essere usati dai soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555. Tali rischi possono essere connessi, ma non solo, a fattori come la giurisdizione applicabile al fabbricante, le caratteristiche della sua proprietà aziendale e i legami di controllo con il governo di un paese terzo in cui esso è stabilito, in particolare se un paese terzo conduce uno spionaggio economico o assume un comportamento irresponsabile nel ciberspazio e se la sua legislazione consente l'accesso arbitrario a qualsiasi tipo di attività o dati aziendali, compresi i dati commercialmente sensibili, e può imporre obblighi a fini di intelligence senza un sistema democratico di bilanciamento dei poteri, meccanismi di controllo, un giusto processo o il diritto di appellarsi a un organo giurisdizionale indipendente. Nel determinare la rilevanza di un rischio di cibersicurezza a norma del presente regolamento, la Commissione e le autorità di vigilanza del mercato, in base alle loro responsabilità stabilite nel presente regolamento, dovrebbero tenere conto anche dei fattori di rischio non tecnici, in

particolare quelli stabiliti a seguito di valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22 della direttiva (UE) 2022/2555.

(59) Al fine di garantire la sicurezza dei prodotti con elementi digitali dopo la loro immissione sul mercato, i fabbricanti dovrebbero stabilire un periodo di assistenza che dovrebbe riflettere il tempo in cui si prevede che il prodotto con elementi digitali rimarrà in uso. Nel determinare un periodo di assistenza, il fabbricante dovrebbe tenere conto in particolare delle ragionevoli aspettative degli utilizzatori, della natura del prodotto e delle pertinenti norme dell'Unione che determinano la durata dei prodotti con elementi digitali. I fabbricanti dovrebbero inoltre poter tenere conto di altri fattori pertinenti. I criteri dovrebbero essere applicati in modo da garantire la proporzionalità nella determinazione del periodo di assistenza. Su richiesta, il fabbricante dovrebbe fornire alle autorità di vigilanza del mercato le informazioni di cui ha tenuto conto nel determinare il periodo di assistenza di un prodotto con elementi digitali.

(60) Il periodo di assistenza durante il quale il fabbricante garantisce la gestione efficace delle vulnerabilità non dovrebbe essere inferiore a cinque anni, a meno che la durata del prodotto con elementi digitali sia inferiore a cinque anni, nel qual caso il fabbricante dovrebbe garantire la gestione delle vulnerabilità per tale durata. Qualora ritengano ragionevolmente che il prodotto con elementi digitali rimarrà in uso per una durata superiore a cinque anni, come spesso avviene nel caso di componenti hardware quali schede madri o microprocessori, dispositivi di rete come router, modem o commutatori, nonché software quali sistemi operativi o strumenti di video-editing, i fabbricanti dovrebbero conseguentemente garantire periodi di assistenza più lunghi. In particolare, i prodotti con elementi digitali destinati a essere utilizzati in contesti industriali, come i sistemi di controllo industriale, restano spesso in uso per periodi di tempo notevolmente superiori. Un fabbricante dovrebbe poter definire un periodo di assistenza inferiore a cinque anni solo se ciò è giustificato dalla natura del prodotto con elementi digitali in questione e se si prevede che tale prodotto sarà utilizzato per meno di cinque anni, nel qual caso il periodo di assistenza dovrebbe corrispondere alla durata di utilizzo prevista. Ad esempio, la durata di un'applicazione per il tracciamento dei contatti destinata ad essere utilizzata durante una pandemia potrebbe essere limitata alla durata di tale pandemia. Inoltre, alcune applicazioni software possono, per loro natura, essere messe a disposizione solo sulla base di un modello di abbonamento, in particolare quando l'applicazione diventa indisponibile per l'utilizzatore e di conseguenza non è più in uso alla scadenza dell'abbonamento.

(61) Per garantire la gestione delle vulnerabilità una volta terminato il periodo di assistenza dei prodotti con elementi digitali, i fabbricanti dovrebbero prendere in considerazione la possibilità di divulgare il codice sorgente di tali prodotti con elementi digitali ad altre imprese che si impegnano a prolungare la prestazione di servizi di gestione delle vulnerabilità oppure al pubblico. Qualora divulghino il codice sorgente ad altre imprese, i fabbricanti dovrebbero poter proteggere la titolarità del prodotto con elementi digitali e impedire la diffusione del codice sorgente al pubblico, ad esempio mediante accordi contrattuali.

(62) Per far sì che i fabbricanti in tutta l'Unione prevedano periodi di assistenza simili per prodotti con elementi digitali comparabili, l'ADCO dovrebbe pubblicare statistiche sui periodi di assistenza medi stabiliti dai fabbricanti per le categorie di prodotti con elementi digitali e divulgare orientamenti che indichino i periodi di assistenza adeguati per tali categorie. Inoltre, al fine di garantire un approccio armonizzato in tutto il mercato interno, la Commissione dovrebbe poter adottare atti delegati per specificare i periodi minimi di assistenza per determinate categorie di prodotti qualora i dati forniti dalle autorità di vigilanza del mercato suggeriscano che i periodi di assistenza stabiliti dai fabbricanti si discostano sistematicamente dai criteri per la determinazione dei periodi di assistenza stabiliti nel presente regolamento o che i fabbricanti di diversi Stati membri determinano periodi di assistenza diversi senza valido motivo.

(63) I fabbricanti dovrebbero istituire un punto di contatto unico che consenta agli utilizzatori di comunicare facilmente con loro, anche al fine di segnalare le vulnerabilità del prodotto con elementi digitali e di ricevere informazioni su tali vulnerabilità. Essi dovrebbero far sì che il punto di contatto sia facilmente accessibile agli utilizzatori, indicandone chiaramente la disponibilità e mantenendo aggiornate le relative informazioni. Se scelgono di offrire strumenti automatizzati, ad esempio chat box, i fabbricanti dovrebbero mettere a disposizione anche un numero di telefono o altri mezzi di contatto digitali, come un indirizzo di posta elettronica o un modulo di contatto. Il punto di contatto unico non dovrebbe basarsi esclusivamente su strumenti automatizzati.

(64) I fabbricanti dovrebbero mettere a disposizione sul mercato i loro prodotti con elementi digitali con una configurazione sicura per impostazione predefinita e fornire gratuitamente gli aggiornamenti di sicurezza agli utilizzatori. I fabbricanti dovrebbero potersi discostare dai requisiti essenziali di cibersicurezza solo nel caso di prodotti su misura installati per uno scopo particolare e per un determinato utilizzatore commerciale e solo se il fabbricante e l'utilizzatore hanno esplicitamente concordato un insieme diverso di clausole contrattuali.

(65) I fabbricanti dovrebbero notificare simultaneamente al team di risposta agli incidenti di sicurezza informatica (*computer security incident response team* - CSIRT) designato come coordinatore e all'ENISA, attraverso la piattaforma unica di segnalazione, le vulnerabilità attivamente sfruttate contenute nei prodotti con elementi digitali come pure gli incidenti gravi che hanno un impatto sulla sicurezza di tali prodotti. Le notifiche dovrebbero essere trasmesse utilizzando il terminale per la notifica elettronica di un CSIRT designato come coordinatore e dovrebbero essere contemporaneamente accessibili all'ENISA.

(66) I fabbricanti dovrebbero notificare le vulnerabilità attivamente sfruttate per garantire che i CSIRT designati come coordinatori e l'ENISA dispongano di una panoramica adeguata di tali vulnerabilità e ricevano le informazioni necessarie per svolgere i loro compiti di cui alla direttiva (UE) 2022/2555 e innalzare il livello generale di cibersicurezza dei soggetti essenziali e importanti di cui all'articolo 3 di tale direttiva, nonché per garantire il funzionamento efficace delle autorità di vigilanza del mercato. Poiché la maggior parte dei prodotti con elementi digitali è commercializzata sull'intero mercato interno, qualsiasi vulnerabilità sfruttata in un prodotto con elementi digitali dovrebbe essere considerata una minaccia al funzionamento del mercato interno. L'ENISA, di comune accordo con il fabbricante, dovrebbe divulgare le vulnerabilità risolte alla banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555. La banca dati europea delle vulnerabilità aiuterà i fabbricanti a individuare le vulnerabilità note sfruttabili riscontrate nei loro prodotti, al fine di garantire l'immissione sul mercato di prodotti sicuri.

(67) I fabbricanti dovrebbero anche notificare qualsiasi incidente grave che abbia un impatto sulla sicurezza del prodotto con elementi digitali al CSIRT designato come coordinatore e all'ENISA. Per far sì che gli utilizzatori possano reagire rapidamente agli incidenti gravi che hanno un impatto sulla sicurezza dei loro prodotti con elementi digitali, i fabbricanti dovrebbero inoltre informare gli utilizzatori di tali incidenti e, se del caso, di eventuali misure correttive che gli utilizzatori potrebbero adottare per attenuarne l'impatto, ad esempio attraverso la pubblicazione di informazioni pertinenti sui propri siti web o il contatto diretto, qualora il fabbricante sia in grado di contattare gli utilizzatori e ciò sia giustificato dai rischi di cibersicurezza.

(68) Con vulnerabilità attivamente sfruttate si indicano casi in cui un fabbricante ha stabilito che una violazione della sicurezza commessa a scapito dei suoi utilizzatori o di qualsiasi altra persona fisica o giuridica è imputabile a un soggetto malintenzionato, il quale ha sfruttato un difetto a livello di uno dei prodotti con elementi digitali messi a disposizione sul mercato dal fabbricante. Tali vulnerabilità possono comprendere ad esempio carenze nelle funzioni di identificazione e autenticazione di un prodotto. Le vulnerabilità individuate senza intento doloso e a scopo di prova, indagine, correzione o divulgazione in buona fede per promuovere la sicurezza del proprietario del sistema e dei suoi utilizzatori non dovrebbero essere soggette a notifica obbligatoria. Gli incidenti gravi che hanno un impatto sulla sicurezza del prodotto con elementi digitali si riferiscono invece a situazioni in cui un incidente di cibersicurezza influisce sui processi di sviluppo, produzione o manutenzione del fabbricante in modo tale da comportare un potenziale aumento del rischio di cibersicurezza per gli utilizzatori o altre persone. Tra gli esempi di incidenti gravi rientra ad esempio il caso di un soggetto malintenzionato che sia riuscito a inserire codice maligno nel canale di diffusione tramite il quale il fabbricante rilascia gli aggiornamenti di sicurezza agli utilizzatori.

(69) Per garantire la diffusione rapida delle notifiche a tutti i CSIRT pertinenti designati come coordinatori e per consentire ai fabbricanti di trasmettere una sola notifica in ogni fase del processo di notifica, l'ENISA dovrebbe istituire una piattaforma unica di segnalazione con terminali per la notifica elettronica a livello nazionale. Le operazioni quotidiane della piattaforma unica di segnalazione dovrebbero essere gestite e mantenute dall'ENISA. I CSIRT designati come coordinatori dovrebbero informare le rispettive autorità di vigilanza del mercato in merito alle vulnerabilità o agli incidenti notificati. La piattaforma unica di segnalazione dovrebbe essere progettata in modo da garantire la riservatezza delle notifiche, specie per quanto riguarda le vulnerabilità per le quali non è ancora disponibile un aggiornamento di sicurezza. Inoltre, l'ENISA dovrebbe attuare procedure che permettano di trattare le informazioni in modo sicuro e riservato. Sulla base delle informazioni raccolte, l'ENISA dovrebbe preparare una relazione tecnica biennale sulle tendenze emergenti relative ai rischi di cibersicurezza nei prodotti con elementi digitali e presentarla al gruppo di cooperazione istituito a norma dell'articolo 14 della direttiva (UE) 2022/2555.

(70) In circostanze eccezionali e in particolare su richiesta del fabbricante, il CSIRT designato come coordinatore che ha ricevuto per primo una notifica dovrebbe avere la facoltà di decidere di ritardarne la diffusione agli altri CSIRT pertinenti designati come coordinatori attraverso la piattaforma unica di segnalazione, se ciò può essere giustificato da motivi connessi alla cibersicurezza e per il periodo di tempo strettamente necessario. Il CSIRT designato come coordinatore dovrebbe informare immediatamente l'ENISA in merito alla decisione di ritardare la diffusione e ai relativi motivi, indicando inoltre il momento in cui intende procedere con l'ulteriore diffusione. La Commissione dovrebbe elaborare, mediante un atto delegato, specifiche sui termini e sulle condizioni per l'eventuale applicazione di motivi connessi alla cibersicurezza e dovrebbe cooperare con la rete di CSIRT istituita a norma dell'articolo 15 della direttiva (UE) 2022/2555 e con l'ENISA nella preparazione del progetto di atto delegato. Tra gli esempi di motivi connessi alla cibersicurezza figurano il fatto che vi sia una procedura di divulgazione coordinata delle vulnerabilità in corso o situazioni in cui un fabbricante è tenuto a fornire una misura di attenuazione in tempi brevi e i rischi di cibersicurezza derivanti da una diffusione immediata attraverso la piattaforma unica di segnalazione

superano i benefici. Se richiesto dal CSIRT designato come coordinatore, l'ENISA dovrebbe essere poter sostenerlo nell'applicazione i motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione della notifica sulla base delle informazioni che l'ENISA ha ricevuto da tale CSIRT in merito alla decisione di trattenere la notifica per tali motivi di cibersicurezza. Inoltre, in circostanze particolarmente eccezionali, l'ENISA non dovrebbe ricevere simultaneamente tutti i dettagli della notifica di una vulnerabilità attivamente sfruttata. Si pensi ad esempio a una situazione in cui il fabbricante ha indicato nella notifica che la vulnerabilità notificata è stata attivamente sfruttata da un soggetto malintenzionato ma, in base alle informazioni disponibili, non è stata sfruttata in altri Stati membri oltre a quello del CSIRT designato come coordinatore al quale il fabbricante ha notificato la vulnerabilità, e laddove un'ulteriore diffusione immediata della vulnerabilità notificata comporterebbe probabilmente la fornitura di informazioni la cui divulgazione sarebbe contraria agli interessi essenziali di tale Stato membro o laddove l'ulteriore diffusione della vulnerabilità notificata si tradurrebbe in un rischio di cibersicurezza elevato e imminente. In tali situazioni, l'ENISA riceverà l'accesso simultaneo unicamente all'informazione dell'avvenuta notifica da parte del fabbricante, alle informazioni generali sul prodotto con elementi digitali in questione, alle informazioni sulla natura generale dello sfruttamento e alla comunicazione del fatto che il fabbricante ha sollevato tali motivi di sicurezza e ha pertanto trattenuto il contenuto integrale della notifica. La notifica completa dovrebbe quindi essere messa a disposizione dell'ENISA e degli altri CSIRT pertinenti designati come coordinatori nel momento in cui il CSIRT designato come coordinatore che ha ricevuto la notifica per primo constata che tali motivi di sicurezza, che riflettono circostanze particolarmente eccezionali come stabilito nel presente regolamento, cessano di esistere. Se, sulla base delle informazioni disponibili, ritiene che vi sia un rischio sistemico capace di incidere sulla sicurezza del mercato interno, l'ENISA dovrebbe raccomandare al CSIRT ricevente di diffondere la notifica completa agli altri CSIRT designati come coordinatori e all'ENISA stessa.

(71) Quando notificano una vulnerabilità attivamente sfruttata o un incidente grave che ha un impatto sulla sicurezza del prodotto con elementi digitali, i fabbricanti dovrebbero indicare il grado di sensibilità da loro attribuito alle informazioni notificate. Il CSIRT designato come coordinatore che ha ricevuto la notifica per primo dovrebbe tenere conto di tali informazioni nel valutare se la notifica dia luogo a circostanze eccezionali tali da giustificare un ritardo nella diffusione della notifica agli altri CSIRT pertinenti designati come coordinatori sulla base di giustificati motivi connessi alla cibersicurezza. Dovrebbe inoltre tenere conto di tali informazioni nel valutare se la notifica di una vulnerabilità attivamente sfruttata dia luogo a circostanze particolarmente eccezionali tali da giustificare il rifiuto di mettere a disposizione dell'ENISA la notifica completa simultaneamente. Infine, i CSIRT designati come coordinatori dovrebbero poter tenere conto di tali informazioni nel determinare le misure appropriate per attenuare i rischi derivanti da tali vulnerabilità e incidenti.

(72) Al fine di semplificare la segnalazione delle informazioni richieste a norma del presente regolamento, tenuto conto degli altri obblighi di segnalazione complementari stabiliti dal diritto dell'Unione, quali il regolamento (UE) 2016/679, il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio ([25]), la direttiva n. 2002/58/CE del Parlamento europeo e del Consiglio ([26]) e la direttiva (UE) 2022/2555, e al fine di ridurre gli oneri amministrativi per i soggetti, gli Stati membri sono incoraggiati a valutare la possibilità di istituire punti di accesso unici a livello nazionale per tali obblighi di comunicazione. L'uso di tali punti di accesso unici a livello nazionale per la segnalazione di incidenti di sicurezza a norma del regolamento (UE) 2016/679 e della direttiva 2002/58/CE non dovrebbe pregiudicare l'applicazione delle disposizioni di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE, in particolare quelle relative all'indipendenza delle autorità ivi menzionate. Nell'istituire la piattaforma unica di segnalazione di cui al presente regolamento, l'ENISA dovrebbe tenere conto della possibilità che i terminali per la notifica elettronica a livello nazionale di cui al presente regolamento siano integrati nei punti di accesso unici nazionali, che possono anche integrare altre notifiche richieste dal diritto dell'Unione.

(73) Nell'istituire la piattaforma unica di segnalazione di cui al presente regolamento e al fine di beneficiare dell'esperienza passata, l'ENISA dovrebbe consultare altre istituzioni o agenzie dell'Unione che gestiscono piattaforme o banche dati soggette a rigorosi requisiti di sicurezza, come l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA). L'ENISA dovrebbe inoltre esaminare le potenziali complementarità con la banca dati europea delle vulnerabilità istituita a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555.

(74) I fabbricanti e le altre persone fisiche e giuridiche dovrebbero poter notificare a un CSIRT designato come coordinatore o all'ENISA, su base volontaria, qualsiasi vulnerabilità contenuta in un prodotto con elementi digitali,

([25]) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).

([26]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (GU L 201 del 31.7.2002, pag. 37).

qualsiasi minaccia informatica che potrebbe incidere sul profilo di rischio di un prodotto con elementi digitali, qualsiasi incidente che abbia un impatto sulla sicurezza del prodotto con elementi digitali nonché qualsiasi quasi incidente che avrebbe potuto tradursi in un simile incidente.

(75) Gli Stati membri dovrebbero mirare ad affrontare, nella misura del possibile, le sfide incontrate dagli esperti che fanno ricerca sulle vulnerabilità, compresa la loro potenziale esposizione alla responsabilità penale, conformemente al diritto nazionale. Dato che in alcuni Stati membri le persone fisiche e giuridiche che fanno ricerca sulle vulnerabilità potrebbero essere esposte alla responsabilità penale e civile, gli Stati membri sono incoraggiati ad adottare orientamenti per quanto riguarda la non perseguibilità dei ricercatori in materia di sicurezza delle informazioni e l'esenzione dalla responsabilità civile per le loro attività.

(76) I fabbricanti di prodotti con elementi digitali dovrebbero mettere in atto politiche di divulgazione coordinata delle vulnerabilità per facilitare la segnalazione delle vulnerabilità da parte di individui o soggetti direttamente al fabbricante o indirettamente e, qualora sia richiesto di procedere in forma anonima, tramite i CSIRT designati come coordinatori ai fini della divulgazione coordinata delle vulnerabilità a norma dell'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555. La politica di divulgazione coordinata delle vulnerabilità dei fabbricanti dovrebbe indicare un processo strutturato attraverso il quale le vulnerabilità sono segnalate al fabbricante in modo da consentire a quest'ultimo di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano comunicate a terzi o al pubblico. Inoltre, i fabbricanti dovrebbero prendere in considerazione la possibilità di pubblicare le loro politiche di sicurezza in un formato leggibile da un dispositivo automatico. Dato che le informazioni sulle vulnerabilità sfruttabili in prodotti con elementi digitali di largo consumo possono essere vendute a prezzi elevati sul mercato nero, i fabbricanti di tali prodotti, nell'ambito delle loro politiche di divulgazione coordinata delle vulnerabilità, dovrebbero poter utilizzare programmi volti a incentivare la segnalazione delle vulnerabilità garantendo che individui o soggetti ricevano un riconoscimento e un compenso per i loro sforzi. Si tratta dei cosiddetti «programmi di bug bounty».

(77) Per facilitare l'analisi delle vulnerabilità, i fabbricanti dovrebbero individuare e documentare i componenti contenuti nei prodotti con elementi digitali, creando anche una distinta base del software. Una distinta base del software può fornire a coloro che realizzano, acquistano e utilizzano il software informazioni che migliorano la loro comprensione della catena di approvvigionamento, con molteplici vantaggi, in particolare quello di aiutare i fabbricanti e gli utilizzatori a tenere traccia delle vulnerabilità e dei rischi di cibersicurezza. È particolarmente importante che i fabbricanti garantiscano che i loro prodotti con elementi digitali non contengono componenti vulnerabili sviluppati da terzi. I fabbricanti non dovrebbero essere obbligati a rendere pubblica la distinta base del software.

(78) Nell'ambito dei nuovi e complessi modelli aziendali legati alle vendite online, un'impresa operante online può fornire una molteplicità di servizi. A seconda della natura dei servizi forniti in relazione a un determinato prodotto con elementi digitali, lo stesso soggetto può rientrare in diverse categorie di modelli aziendali o operatori economici. Se un soggetto fornisce solo servizi di intermediazione online per un dato prodotto con elementi digitali ed è unicamente un fornitore di un mercato online quale definito all'articolo 3, paragrafo 14, del regolamento (UE) 2023/988, tale soggetto non rientra in una delle tipologie di operatore economico di cui al presente regolamento. Qualora lo stesso soggetto sia un fornitore di un mercato online e agisca anche in qualità di operatore economico quale definito nel presente regolamento per la vendita di prodotti con elementi digitali, esso dovrebbe essere soggetto agli obblighi di cui al presente regolamento per quel tipo di operatore economico. Ad esempio, se il fornitore di un mercato online distribuisce anche un prodotto con elementi digitali, ai fini della vendita di tale prodotto sarebbe considerato un distributore. Parimenti, se il soggetto in questione vendesse i prodotti con elementi digitali con il proprio marchio, sarebbe considerato fabbricante e dovrebbe quindi rispettare i requisiti applicabili ai fabbricanti. Inoltre, alcuni soggetti possono essere considerati fornitori di servizi di logistica a norma dell'articolo 3, paragrafo 11, del regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio ([27]), se offrono tali servizi. Si tratta di casi che vanno valutati individualmente. Dato il ruolo di primo piano svolto dai mercati online nel consentire il commercio elettronico, essi dovrebbero adoperarsi per cooperare con le autorità di vigilanza del mercato degli Stati membri al fine di aiutare a garantire che i prodotti con elementi digitali acquistati attraverso mercati online siano conformi ai requisiti di cibersicurezza di cui al presente regolamento.

(79) Al fine di facilitare la valutazione della conformità ai requisiti stabiliti dal presente regolamento, è opportuno che vi sia una presunzione di conformità per i prodotti con elementi digitali conformi alle norme armonizzate che traducono i requisiti essenziali di cibersicurezza stabiliti nel presente regolamento in specifiche tecniche dettagliate

([27]) 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 (GU L 169 del 25.6.2019, pag. 1).

e che sono adottate conformemente al regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([28]). Tale regolamento prevede una procedura di obiezione a norme armonizzate che non soddisfano completamente i requisiti stabiliti nel presente regolamento. Il processo di normazione dovrebbe garantire una rappresentazione equilibrata degli interessi e un'effettiva partecipazione dei portatori di interessi della società civile, comprese le organizzazioni dei consumatori. È opportuno tenere conto anche delle norme internazionali allineate con il livello di protezione della cibersicurezza perseguito dai requisiti essenziali di cibersicurezza di cui al presente regolamento, al fine di agevolare l'elaborazione di norme armonizzate e l'attuazione del presente regolamento, nonché di agevolare la conformità per le imprese, in particolare le microimprese e le piccole e medie imprese e quelle che operano a livello mondiale.

(80) L'elaborazione tempestiva di norme armonizzate durante il periodo di transizione per l'applicazione del presente regolamento e la loro disponibilità prima della data di applicazione del presente regolamento saranno particolarmente importanti per la sua effettiva attuazione. Ciò vale in modo particolare per i prodotti con elementi digitali importanti rientranti nella classe I. La disponibilità di norme armonizzate consentirà ai fabbricanti di tali prodotti di effettuare le valutazioni della conformità attraverso la procedura di controllo interno e può pertanto evitare strozzature e ritardi nelle attività degli organismi di valutazione della conformità.

(81) Il regolamento (UE) 2019/881 istituisce un quadro volontario europeo di certificazione della cibersicurezza per i prodotti, i servizi e i processi TIC. I sistemi europei di certificazione della cibersicurezza forniscono un quadro comune di fiducia per gli utilizzatori dei prodotti con elementi digitali rientranti nell'ambito del presente regolamento. Il presente regolamento dovrebbe pertanto creare sinergie con il regolamento (UE) 2019/881. Al fine di facilitare la valutazione della conformità ai requisiti stabiliti nel presente regolamento, i prodotti con elementi digitali che sono certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema di cibersicurezza europeo a norma del regolamento (UE) 2019/881 che sia stato identificato dalla Commissione in un atto di esecuzione sono considerati conformi ai requisiti essenziali di cibersicurezza di cui al presente regolamento nella misura in cui tali requisiti siano contemplati nel certificato di cibersicurezza o nella dichiarazione di conformità europei o in parti di essi. La necessità di nuovi sistemi europei di certificazione della cibersicurezza per i prodotti con elementi digitali dovrebbe essere valutata alla luce del presente regolamento, anche nell'ambito della preparazione del programma di lavoro progressivo dell'Unione a norma del regolamento (UE) 2019/881. Qualora si renda necessario un nuovo sistema per i prodotti con elementi digitali, anche al fine di agevolare il rispetto del presente regolamento, la Commissione può chiedere all'ENISA di preparare proposte di sistemi conformemente all'articolo 48 del regolamento (UE) 2019/881. Tali futuri sistemi europei di certificazione della cibersicurezza relativi ai prodotti con elementi digitali dovrebbero tenere conto dei requisiti essenziali di cibersicurezza e delle procedure di valutazione della conformità stabiliti nel presente regolamento e facilitare la conformità a quest'ultimo. Per i sistemi europei di certificazione della cibersicurezza che entrano in vigore prima dell'entrata in vigore del presente regolamento, possono rendersi necessarie ulteriori specifiche su aspetti particolari delle modalità di applicazione della presunzione di conformità. Alla Commissione dovrebbe essere conferito il potere di specificare, mediante atti delegati, a quali condizioni i sistemi europei di certificazione della cibersicurezza possono essere utilizzati per dimostrare la conformità ai requisiti essenziali di cibersicurezza stabiliti nel presente regolamento. Inoltre, onde evitare un onere amministrativo indebito a carico dei fabbricanti, non dovrebbe esistere alcun obbligo per i fabbricanti di effettuare una valutazione della conformità da parte di terzi, come previsto dal presente regolamento per i requisiti corrispondenti, se è stato rilasciato un certificato di cibersicurezza europeo nell'ambito di tali sistemi europei di certificazione della cibersicurezza con un livello almeno «sostanziale».

(82) All'entrata in vigore del regolamento di esecuzione (UE) 2024/482 che riguarda i prodotti rientranti nell'ambito del presente regolamento, come i microprocessori e i moduli di sicurezza dell'hardware, la Commissione dovrebbe essere poter specificare, mediante un atto delegato, come tale sistema conferisca una presunzione di conformità ai requisiti essenziali di cibersicurezza di cui al presente regolamento o a sue parti. Inoltre tale atto delegato può specificare in che modo un certificato rilasciato nell'ambito del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni sopprima l'obbligo per i fabbricanti di effettuare una valutazione da parte di terzi, come previsto a norma del presente regolamento per i requisiti corrispondenti.

(83) L'attuale quadro europeo in materia di normalizzazione, basato sui principi della nuova strategia stabiliti nella risoluzione del Consiglio, del 7 maggio 1985, relativa ad una nuova strategia in materia di armonizzazione tecnica e normalizzazione e sul regolamento (UE) n. 1025/2012, rappresenta il quadro predefinito per l'elaborazione di norme che conferiscano una presunzione di conformità ai pertinenti requisiti essenziali di cibersicurezza di cui al presente regolamento. Le norme europee dovrebbero essere orientate al mercato e tenere conto dell'interesse pubblico, nonché degli obiettivi strategici chiaramente indicati nella richiesta della Commissione a una o più organizzazioni europee di normazione di elaborare norme armonizzate entro un termine stabilito, ed essere basate sul consenso. Tuttavia, in assenza di riferimenti pertinenti a norme armonizzate, la Commissione dovrebbe poter

([28]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

adottare atti di esecuzione che stabiliscano specifiche comuni per i requisiti essenziali di cibersicurezza previsti dal presente regolamento, a condizione che nel farlo rispetti debitamente il ruolo e le funzioni delle organizzazioni europee di normazione, quale soluzione eccezionale di ripiego per facilitare l'obbligo del fabbricante di rispettare tali requisiti essenziali di cibersicurezza, laddove il processo di normazione sia bloccato o vi siano ritardi nella definizione di norme armonizzate appropriate. Se tale ritardo è dovuto alla complessità tecnica della norma in questione, la Commissione dovrebbe tenerne conto prima di prendere in considerazione l'eventuale definizione di specifiche comuni.

(84) Al fine di stabilire, nel modo più efficiente possibile, specifiche comuni che contemplino i requisiti essenziali di cibersicurezza di cui al presente regolamento, la Commissione dovrebbe coinvolgere nel processo le parti interessate.

(85) Per «termine ragionevole» si intende, in relazione alla pubblicazione del riferimento alle norme armonizzate nella *Gazzetta ufficiale dell'Unione europea* conformemente al regolamento (UE) n. 1025/2012, un periodo di tempo durante il quale è prevista la pubblicazione nella *Gazzetta ufficiale dell'Unione europea* del riferimento alla norma, alla sua rettifica o alla sua modifica e che non dovrebbe superare un anno dal termine per l'elaborazione di un insieme di norme europee fissato conformemente al regolamento (UE) n. 1025/2012.

(86) Per facilitare la valutazione della conformità ai requisiti essenziali di cibersicurezza stabiliti dal presente regolamento, è opportuno che vi sia una presunzione di conformità per i prodotti con elementi digitali conformi alle specifiche comuni adottate dalla Commissione a norma del presente regolamento al fine della formulazione di specifiche tecniche dettagliate in relazione a tali requisiti.

(87) L'applicazione di norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che conferiscono una presunzione di conformità in relazione ai requisiti essenziali di cibersicurezza applicabili ai prodotti con elementi digitali faciliterà la valutazione della conformità da parte dei fabbricanti. Se sceglie di non applicare tali mezzi per determinati requisiti, il fabbricante deve indicare nella documentazione tecnica in quale altro modo viene raggiunta la conformità. Inoltre, l'applicazione di norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che conferiscono una presunzione di conformità da parte dei fabbricanti faciliterebbe il controllo della conformità dei prodotti con elementi digitali da parte delle autorità di vigilanza del mercato. I fabbricanti di prodotti con elementi digitali sono pertanto incoraggiati ad applicare tali norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza.

(88) I fabbricanti dovrebbero redigere una dichiarazione di conformità UE che fornisca le informazioni richieste a norma del presente regolamento sulla conformità dei prodotti con elementi digitali ai requisiti essenziali di cibersicurezza stabiliti dal presente regolamento e, ove applicabile, da altri atti pertinenti della normativa di armonizzazione dell'Unione che disciplinano tale prodotto con elementi digitali. I fabbricanti possono altresì essere tenuti a redigere una dichiarazione di conformità UE in base ad altri atti giuridici dell'Unione. Al fine di garantire un accesso efficace alle informazioni per fini di vigilanza del mercato, dovrebbe essere redatta un'unica dichiarazione di conformità UE per quanto riguarda la conformità a tutti gli atti giuridici pertinenti dell'Unione. Al fine di ridurre l'onere amministrativo a carico degli operatori economici, tale dichiarazione di conformità UE unica dovrebbe poter consistere in un fascicolo comprendente le dichiarazioni di conformità individuali pertinenti.

(89) La marcatura CE, che indica la conformità di un prodotto, è la conseguenza visibile di un intero processo che comprende la valutazione della conformità in senso lato. I principi generali che disciplinano la marcatura CE sono indicati nel regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio ([29]). È opportuno che nel presente regolamento siano fissate le norme relative all'apposizione della marcatura CE sui prodotti con elementi digitali. La marcatura CE dovrebbe essere l'unica marcatura che garantisce la conformità dei prodotti con elementi digitali ai requisiti stabiliti dal presente regolamento.

(90) Per consentire agli operatori economici di dimostrare la conformità ai requisiti essenziali di cibersicurezza stabiliti nel presente regolamento e alle autorità di vigilanza del mercato di garantire che i prodotti con elementi digitali messi a disposizione sul mercato siano conformi a tali requisiti, è necessario prevedere procedure di valutazione della

([29]) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che fissa le norme in materia di accreditamento e abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

conformità. La decisione n. 768/2008/CE del Parlamento europeo e del Consiglio ([30]) stabilisce moduli per le procedure di valutazione della conformità proporzionalmente al livello di rischio effettivo e di sicurezza richiesto. Per garantire la coerenza intersettoriale ed evitare varianti ad hoc, le procedure di valutazione della conformità adeguate per verificare la conformità dei prodotti con elementi digitali ai requisiti essenziali di cibersicurezza stabiliti nel presente regolamento dovrebbero essere basate su tali moduli. Le procedure di valutazione della conformità dovrebbero esaminare e verificare sia i requisiti relativi al prodotto sia quelli relativi al processo riguardanti l'intero ciclo di vita dei prodotti con elementi digitali, tra cui la pianificazione, la progettazione, lo sviluppo o la produzione, il collaudo e la manutenzione del prodotto con elementi digitali.

(91) La valutazione della conformità dei prodotti con elementi digitali che non sono elencati come prodotti con elementi digitali importanti o critici nel presente regolamento può essere effettuata dal fabbricante sotto la propria responsabilità, applicando la procedura di controllo interno basata sul modulo A della decisione n. 768/2008/CE conformemente al presente regolamento. Ciò si applica anche ai casi in cui un fabbricante sceglie di non applicare, in tutto o in parte, una norma armonizzata, una specifica comune o un sistema europeo di certificazione della cibersicurezza applicabili. Il fabbricante mantiene la flessibilità di scegliere una procedura di valutazione della conformità più rigorosa che coinvolga terzi. Nell'ambito della procedura di valutazione della conformità di controllo interno, il fabbricante garantisce e dichiara, sotto la propria esclusiva responsabilità, che il prodotto con elementi digitali e i processi messi in atto dal fabbricante soddisfano i requisiti essenziali di cibersicurezza applicabili di cui al presente regolamento. Se un prodotto con elementi digitali importante rientra nella classe I, è necessaria una garanzia supplementare per dimostrare la conformità ai requisiti essenziali di cibersicurezza stabiliti nel presente regolamento. Se intende effettuare la valutazione della conformità sotto la propria responsabilità (modulo A), il fabbricante dovrebbe applicare le norme armonizzate, le specifiche comuni o i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che sono stati identificati dalla Commissione in un atto di esecuzione. Se non applica tali norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza, il fabbricante dovrebbe effettuare una valutazione della conformità che coinvolga terzi (basata sui moduli B e C o sul modulo H). Tenendo conto dell'onere amministrativo a carico dei fabbricanti e del fatto che la cibersicurezza svolge un ruolo importante nella fase di progettazione e sviluppo dei prodotti tangibili e intangibili con elementi digitali, le procedure di valutazione della conformità basate sui moduli B e C o sul modulo H della decisione 768/2008/CE sono state scelte come le più appropriate per valutare la conformità dei prodotti con elementi digitali importanti in modo proporzionato ed efficace. Il fabbricante che effettua la valutazione della conformità da parte di terzi può scegliere la procedura che meglio si adatta al suo processo di progettazione e produzione. Dato il rischio di cibersicurezza ancora maggiore legato all'uso di prodotti con elementi digitali importanti che rientrano nella classe II, la valutazione della conformità dovrebbe sempre coinvolgere terzi, anche se il prodotto è pienamente o parzialmente conforme alle norme armonizzate, alle specifiche comuni o ai sistemi europei di certificazione della cibersicurezza. I fabbricanti di prodotti con elementi digitali importanti che si qualificano come software liberi e open source dovrebbero essere poter seguire la procedura di controllo interno basata sul modulo A, a condizione che mettano la documentazione tecnica a disposizione del pubblico.

(92) Mentre la creazione di prodotti tangibili con elementi digitali richiede di norma un notevole impegno da parte dei fabbricanti nelle fasi di progettazione, sviluppo e produzione, la creazione di prodotti con elementi digitali sotto forma di software si concentra quasi esclusivamente sulla progettazione e sullo sviluppo, mentre la fase di produzione svolge un ruolo minore. Tuttavia in molti casi i prodotti software devono ancora essere compilati, costruiti, pacchettizzati, messi a disposizione per il download o copiati su supporti fisici prima di essere immessi sul mercato. Tali attività dovrebbero essere considerate attività assimilabili alla produzione quando si applicano i moduli di valutazione della conformità pertinenti per verificare la conformità del prodotto ai requisiti essenziali di cibersicurezza stabiliti dal presente regolamento nelle fasi di progettazione, sviluppo e produzione.

(93) Per quanto riguarda le microimprese e le piccole imprese, al fine di garantire la proporzionalità, è opportuno alleviare i costi amministrativi senza incidere sul livello di protezione della cibersicurezza dei prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento o sulla parità di condizioni tra i fabbricanti. È pertanto opportuno che la Commissione istituisca un modulo di documentazione tecnica semplificata che risponda alle esigenze delle microimprese e delle piccole imprese. Il modulo di documentazione tecnica semplificata adottato dalla Commissione dovrebbe coprire tutti gli elementi applicabili relativi alla documentazione tecnica di cui al presente regolamento e specificare in che modo una microimpresa o una piccola impresa può fornire in modo conciso gli elementi richiesti, come la descrizione della progettazione, dello sviluppo e della produzione del prodotto con elementi digitali. In tal modo, il modulo contribuirebbe ad alleviare gli oneri amministrativi di conformità fornendo alle imprese interessate certezza giuridica circa la portata e la precisione delle informazioni da fornire. Le microimprese e le piccole imprese dovrebbero poter scegliere di fornire gli elementi applicabili relativi alla documentazione tecnica in forma estesa e di non ricorrere al modulo tecnico semplificato a loro disposizione.

([30]) Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE (GU L 218 del 13.8.2008, pag. 82).

(94) Al fine di promuovere e proteggere l'innovazione, è importante che si tenga conto specialmente degli interessi dei fabbricanti che sono microimprese o piccole o medie imprese, in particolare delle microimprese e delle piccole imprese, comprese le start-up. A tal fine, gli Stati membri potrebbero sviluppare iniziative rivolte ai fabbricanti che sono microimprese o piccole imprese, anche in materia di formazione, sensibilizzazione, comunicazione delle informazioni e attività di prova e di valutazione della conformità da parte di terzi, nonché la creazione di spazi di sperimentazione. I costi di traduzione relativi alla documentazione obbligatoria, come la documentazione tecnica e le informazioni e le istruzioni per l'utilizzatore richieste a norma del presente regolamento, nonché alla comunicazione con le autorità, possono costituire un costo significativo per i fabbricanti, specie per quelli di dimensioni minori. Gli Stati membri dovrebbero pertanto poter prevedere che una delle lingue da essi indicate e accettate per la documentazione dei fabbricanti pertinenti e per la comunicazione con i fabbricanti sia una lingua ampiamente compresa dal maggior numero possibile di utilizzatori.

(95) Al fine di garantire la corretta applicazione del presente regolamento, gli Stati membri dovrebbero adoperarsi per garantire, prima della sua data di applicazione, che sia disponibile un numero sufficiente di organismi notificati per eseguire le valutazioni della conformità da parte di terzi. La Commissione dovrebbe cercare di assistere gli Stati membri e le altre parti interessate in tale sforzo, al fine di evitare strozzature e ostacoli all'ingresso sul mercato dei fabbricanti. Le attività di formazione mirate condotte dagli Stati membri, se del caso anche con il sostegno della Commissione, possono contribuire alla disponibilità di professionisti qualificati, anche a sostegno delle attività degli organismi notificati a norma del presente regolamento. Inoltre, alla luce dei costi che la valutazione della conformità da parte di terzi può comportare, è opportuno prendere in considerazione iniziative di finanziamento a livello nazionale e dell'Unione volte ad alleviare tali costi per le microimprese e le piccole imprese.

(96) Al fine di garantire la proporzionalità, gli organismi di valutazione della conformità, nel fissare le tariffe per le procedure di valutazione della conformità, dovrebbero tenere conto degli interessi e delle esigenze specifici delle microimprese e delle piccole e medie imprese, comprese le start-up. In particolare, gli organismi di valutazione della conformità dovrebbero applicare la procedura d'esame e le prove pertinenti di cui al presente regolamento solo ove opportuno e seguendo un approccio basato sul rischio.

(97) L'obiettivo degli spazi di sperimentazione normativa dovrebbe essere quello di promuovere l'innovazione e la competitività delle imprese, istituendo ambienti di prova controllati prima dell'immissione sul mercato di prodotti con elementi digitali. Gli spazi di sperimentazione normativa dovrebbero contribuire a migliorare la certezza del diritto per tutti gli attori che rientrano nell'ambito di applicazione del presente regolamento, nonché ad agevolare e accelerare l'accesso al mercato dell'Unione dei prodotti con elementi digitali, in particolare se forniti da microimprese e piccole imprese, comprese le start-up.

(98) Ai fini della valutazione della conformità da parte di terzi dei prodotti con elementi digitali, le autorità nazionali di notifica dovrebbero notificare gli organismi di valutazione della conformità alla Commissione e agli altri Stati membri, a condizione che tali organismi soddisfino una serie di requisiti, in particolare in materia di indipendenza, competenza e assenza di conflitti di interesse.

(99) Per garantire un livello uniforme di qualità nello svolgimento della valutazione della conformità dei prodotti con elementi digitali, è altresì necessario stabilire requisiti da applicare alle autorità di notifica e agli altri organismi che intervengono nella valutazione, nella notifica e nel controllo degli organismi notificati. Il sistema previsto dal presente regolamento dovrebbe essere completato dal sistema di accreditamento di cui al regolamento (CE) n. 765/2008. Poiché l'accreditamento è un mezzo essenziale per la verifica della competenza degli organismi di valutazione della conformità, è opportuno impiegarlo anche ai fini della notifica.

(100) Gli organismi di valutazione della conformità che sono stati accreditati e notificati a norma del diritto dell'Unione che stabilisce requisiti simili a quelli stabiliti nel presente regolamento, come un organismo di valutazione della conformità notificato per un sistema europeo di certificazione della cibersicurezza adottato a norma del regolamento (UE) 2019/881 o notificato a norma del regolamento delegato (UE) 2022/30, dovrebbero essere oggetto di una nuova valutazione e notifica a norma del presente regolamento. Tuttavia, le autorità competenti possono definire sinergie per quanto riguarda eventuali sovrapposizioni di requisiti, al fine di evitare inutili oneri finanziari e amministrativi e di garantire un processo di notifica agevole e tempestivo.

(101) L'accreditamento trasparente, quale previsto dal regolamento (CE) n. 765/2008, che garantisce il necessario livello di fiducia nei certificati di conformità, dovrebbe essere considerato dalle autorità pubbliche nazionali in tutta l'Unione lo strumento preferito per dimostrare la competenza tecnica di tali organismi. Tuttavia le autorità nazionali possono ritenere di possedere gli strumenti idonei a eseguire da sé tale valutazione. In tal caso, onde assicurare l'opportuno livello di credibilità delle valutazioni effettuate dalle altre autorità nazionali, dovrebbero fornire alla Commissione e agli altri Stati membri le necessarie prove documentali che dimostrino che gli organismi di valutazione della conformità valutati rispettano i pertinenti requisiti.

(102) Spesso gli organismi di valutazione della conformità subappaltano parti delle loro attività connesse alla valutazione della conformità o fanno ricorso ad un'affiliata. Al fine di salvaguardare il livello di tutela richiesto per un prodotto con elementi digitali da immettere sul mercato, è indispensabile che i subappaltatori e le affiliate di valutazione della conformità rispettino gli stessi requisiti applicati agli organismi notificati in relazione allo svolgimento di compiti di valutazione della conformità.

(103) La notifica di un organismo di valutazione della conformità dovrebbe essere inviata dall'autorità di notifica alla Commissione e agli altri Stati membri tramite il sistema informativo NANDO (*New Approach Notified and Designated Organisations*). Il sistema informativo NANDO è lo strumento elettronico di notifica elaborato e gestito dalla Commissione in cui è possibile trovare un elenco di tutti gli organismi notificati.

(104) Poiché gli organismi notificati possono offrire i propri servizi in tutta l'Unione, è opportuno conferire agli altri Stati membri e alla Commissione la possibilità di sollevare obiezioni relative a un organismo notificato. È pertanto importante prevedere un periodo durante il quale sia possibile chiarire eventuali dubbi o preoccupazioni circa la competenza degli organismi di valutazione della conformità prima che essi inizino ad operare in qualità di organismi notificati.

(105) Nell'interesse della competitività, è fondamentale che gli organismi notificati applichino le procedure di valutazione della conformità senza creare un onere superfluo per gli operatori economici. Analogamente, e per garantire parità di trattamento agli operatori economici dovrebbe essere garantita un'applicazione tecnica coerente delle procedure di valutazione della conformità. Essa dovrebbe essere ottenuta più agevolmente mediante un coordinamento e una cooperazione appropriati tra organismi notificati.

(106) La vigilanza del mercato è un'attività essenziale per garantire l'applicazione corretta ed uniforme del diritto dell'Unione. Di conseguenza è opportuno istituire un quadro giuridico entro il quale la vigilanza del mercato possa svolgersi in maniera adeguata. Le norme sulla vigilanza del mercato dell'Unione e sul controllo dei prodotti che entrano nel mercato dell'Unione di cui al regolamento (UE) 2019/1020 si applicano ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento.

(107) Conformemente al regolamento (UE) 2019/1020, un'autorità di vigilanza del mercato effettua la vigilanza del mercato nel territorio dello Stato membro da cui è designata. Il presente regolamento non dovrebbe impedire agli Stati membri di scegliere le autorità competenti incaricate dello svolgimento dei compiti di vigilanza del mercato. Ogni Stato membro dovrebbe designare una o più autorità di vigilanza del mercato nel proprio territorio. Gli Stati membri dovrebbero poter scegliere di designare qualsiasi autorità già esistente o una nuova autorità che agisca come autorità di vigilanza del mercato, comprese le autorità competenti designate o istituite a norma dell'articolo 8 della direttiva (UE) 2022/2555, le autorità nazionali di certificazione della cibersicurezza designate a norma dell'articolo 58 del regolamento (UE) 2019/881 o le autorità di vigilanza del mercato designate ai fini della direttiva 2014/53/UE. Gli operatori economici dovrebbero collaborare pienamente con le autorità di vigilanza del mercato e con le altre autorità competenti. Ogni Stato membro dovrebbe informare la Commissione e gli altri Stati membri circa le sue autorità di vigilanza del mercato e gli ambiti di competenza di ciascuna autorità e garantire le risorse e le competenze necessarie per svolgere i compiti di vigilanza del mercato relativi al presente regolamento. A norma dell'articolo 10, paragrafi 2 e 3, del regolamento (UE) 2019/1020, ogni Stato membro dovrebbe designare un ufficio unico di collegamento responsabile, tra l'altro, di rappresentare la posizione coordinata delle autorità di vigilanza del mercato e di fornire sostegno alla cooperazione tra le autorità di vigilanza del mercato di diversi Stati membri.

(108) È opportuno istituire un ADCO per la ciberresilienza dei prodotti con elementi digitali per l'applicazione uniforme del presente regolamento, a norma dell'articolo 30, paragrafo 2, del regolamento (UE) 2019/1020. L'ADCO dovrebbe essere composto da rappresentanti delle autorità di vigilanza del mercato designate e, se del caso, da rappresentanti degli uffici unici di collegamento. La Commissione dovrebbe sostenere e incoraggiare la cooperazione tra le autorità di vigilanza del mercato attraverso la rete dell'Unione per la conformità dei prodotti istituita a norma dell'articolo 29 del regolamento (UE) 2019/1020 e composta da rappresentanti di ciascuno Stato membro, inclusi un rappresentante degli uffici unici di collegamento di cui all'articolo 10 di tale regolamento, e un esperto nazionale opzionale, i presidenti degli ADCO e rappresentanti della Commissione. La Commissione dovrebbe partecipare alle riunioni della rete dell'Unione per la conformità dei prodotti, dei suoi sottogruppi e dell'ADCO. Dovrebbe inoltre assistere quest'ultimo attraverso una segreteria esecutiva che fornisce supporto tecnico e logistico. L'ADCO può anche invitare esperti indipendenti a partecipare e mantenere i contatti con altri ADCO, come quello istituito a norma della direttiva 2014/53/UE.

(109) Le autorità di vigilanza del mercato, attraverso l'ADCO istituito a norma del presente regolamento, dovrebbero cooperare strettamente e poter elaborare documenti di orientamento per agevolare le attività di vigilanza del mercato a livello nazionale, ad esempio sviluppando migliori pratiche e indicatori per verificare efficacemente la conformità dei prodotti con elementi digitali al presente regolamento.

(110) Al fine di garantire misure tempestive, proporzionate ed efficaci in relazione ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo, è opportuno prevedere una procedura di salvaguardia dell'Unione in base alla quale le parti interessate siano informate delle misure che si intendono adottare per quanto riguarda tali prodotti. Ciò dovrebbe consentire inoltre alle autorità di vigilanza del mercato, in cooperazione con gli operatori economici interessati, di intervenire in una fase precoce, ove necessario. Nei casi in cui gli Stati membri e la Commissione concordino sul fatto che una misura presa da uno Stato membro sia giustificata, dovrebbero essere previsti ulteriori interventi da parte della Commissione, tranne qualora la non conformità possa essere attribuita a carenze di una norma armonizzata.

(111) In alcuni casi un prodotto con elementi digitali conforme al presente regolamento può tuttavia presentare un rischio di cibersicurezza significativo o comportare un rischio per la salute o la sicurezza delle persone, per la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali, per la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti utilizzando un sistema di informazione elettronico da parte di soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555 o per altri aspetti della tutela dell'interesse pubblico. È quindi necessario stabilire norme che garantiscano l'attenuazione di tali rischi. Di conseguenza le autorità di vigilanza del mercato dovrebbero adottare misure per imporre all'operatore economico di garantire che il prodotto non presenti più tale rischio oppure di richiamarlo o di ritirarlo, a seconda del rischio. Non appena un'autorità di vigilanza del mercato limita o vieta in tal modo la libera circolazione di un prodotto con elementi digitali, lo Stato membro dovrebbe notificare senza indugio alla Commissione e agli altri Stati membri le misure provvisorie, indicando motivi e giustificazioni della decisione. Qualora un'autorità di vigilanza del mercato adotti tali misure contro prodotti con elementi digitali che presentano un rischio, la Commissione dovrebbe avviare senza indugio consultazioni con gli Stati membri e con l'operatore o gli operatori economici interessati e valutare la misura nazionale. In base ai risultati di tale valutazione, la Commissione dovrebbe decidere se la misura nazionale sia giustificata o meno. La Commissione dovrebbe indirizzare la sua decisione a tutti gli Stati membri e comunicarla immediatamente ad essi e all'operatore o agli operatori economici interessati. Se la misura è considerata giustificata, la Commissione dovrebbe anche valutare se adottare proposte per rivedere il pertinente diritto dell'Unione.

(112) Per i prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo e qualora vi sia motivo di ritenere che non siano conformi al presente regolamento o per i prodotti conformi al presente regolamento, ma che presentano altri rischi gravi, quali i rischi per la salute o la sicurezza delle persone, per il rispetto degli obblighi previsti dal diritto dell'Unione o nazionale volti a tutelare i diritti fondamentali o per la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti utilizzando un sistema di informazione elettronico da parte dei soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555, la Commissione dovrebbe poter chiedere all'ENISA di effettuare una valutazione. Sulla base di tale valutazione, la Commissione dovrebbe poter adottare, mediante atti di esecuzione, misure correttive o restrittive a livello dell'Unione, tra cui imporre l'obbligo di ritirare dal mercato o di richiamare i prodotti con elementi digitali interessati, entro un termine ragionevole, proporzionato alla natura del rischio. La Commissione dovrebbe poter ricorrere a tale intervento solo in circostanze eccezionali che giustifichino un intervento immediato per preservare il corretto funzionamento del mercato interno e solo nel caso in cui le autorità di vigilanza del mercato non abbiano adottato misure efficaci per porre rimedio alla situazione. Tali circostanze eccezionali possono essere situazioni di emergenza in cui, ad esempio, il fabbricante mette ampiamente a disposizione, in diversi Stati membri, un prodotto con elementi digitali non conforme che è utilizzato anche in settori essenziali dai soggetti che rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555 e che contiene vulnerabilità note sfruttate da soggetti malintenzionati, per le quali il fabbricante non prevede la disponibilità di patch. La Commissione dovrebbe poter intervenire in tali situazioni di emergenza solo per la durata delle circostanze eccezionali e se la non conformità al presente regolamento o i gravi rischi presentati persistono.

(113) Qualora vi siano indicazioni di non conformità al presente regolamento in diversi Stati membri, le autorità di vigilanza del mercato dovrebbero poter svolgere attività congiunte con altre autorità al fine di verificare la conformità e individuare i rischi di cibersicurezza dei prodotti con elementi digitali.

(114) Le azioni di controllo coordinate e simultanee («indagini a tappeto»), che sono intraprese dalle autorità di vigilanza del mercato con l'obiettivo specifico di controllare l'osservanza delle norme, possono migliorare ulteriormente la sicurezza dei prodotti. In particolare dovrebbero essere condotte indagini a tappeto laddove le tendenze del mercato, i reclami dei consumatori o altri elementi indichino che talune categorie di prodotti con elementi digitali spesso presentano rischi di cibersicurezza. Inoltre, nel determinare le categorie di prodotti da sottoporre a indagini a tappeto, le autorità di vigilanza del mercato dovrebbero tenere conto anche di circostanze relative ai fattori di rischio non tecnici. A tal fine, le autorità di vigilanza del mercato dovrebbero poter tenere conto dei risultati delle valutazioni dei rischi per la sicurezza coordinate a livello di Unione delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22 della direttiva (UE) 2022/2555, comprese le circostanze relative ai fattori di rischio non tecnici. L'ENISA dovrebbe presentare alle autorità di vigilanza del mercato proposte di categorie di prodotti con elementi digitali per le quali potrebbero essere organizzate indagini a tappeto, basandosi, tra l'altro, sulle notifiche ricevute riguardanti le vulnerabilità e gli incidenti.

(115) Alla luce delle sue competenze e il suo mandato, l'ENISA dovrebbe poter sostenere il processo di attuazione del presente regolamento. In particolare, l'ENISA dovrebbe poter proporre attività congiunte che saranno svolte dalle autorità di vigilanza del mercato sulla base di indicazioni o informazioni riguardanti la potenziale non conformità al presente regolamento di prodotti con elementi digitali in diversi Stati membri o di individuare categorie di prodotti per le quali dovrebbero essere organizzati controlli a tappeto. In circostanze eccezionali, su richiesta della Commissione, l'ENISA dovrebbe poter effettuare valutazioni su specifici prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo, qualora sia necessario un intervento immediato per preservare il corretto funzionamento del mercato interno.

(116) Il presente regolamento conferisce all'ENISA taluni compiti che richiedono risorse adeguate, sia in termini di competenze che di risorse umane, per consentirle di svolgere efficacemente tali compiti. In sede di preparazione del progetto di bilancio generale dell'Unione, la Commissione proporrà le necessarie risorse di bilancio per la tabella dell'organico dell'ENISA, conformemente alla procedura di cui all'articolo 29 del regolamento (UE) 2019/881. Nel corso di tale processo, la Commissione prenderà in considerazione le risorse complessive dell'ENISA per consentirle di svolgere i suoi compiti, compresi quelli conferitile a norma del presente regolamento.

(117) Al fine di garantire che il quadro normativo possa essere adattato ove necessario, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea (TFUE) per aggiornare un allegato del presente regolamento che elenca i prodotti con elementi digitali importanti. È opportuno delegare alla Commissione il potere di adottare atti conformemente a tale articolo per individuare i prodotti con elementi digitali disciplinati da altre norme dell'Unione che conseguono lo stesso livello di protezione del presente regolamento, specificando se sia necessaria una limitazione o un'esclusione dall'ambito di applicazione del presente regolamento nonché la portata di tale limitazione, ove applicabile. È opportuno delegare alla Commissione il potere di adottare atti conformemente a tale articolo anche per quanto riguarda l'eventuale obbligo di certificazione nell'ambito di un sistema europeo di certificazione della cibersicurezza dei prodotti con elementi digitali critici in allegato al presente regolamento, nonché per aggiornare l'elenco dei prodotti con elementi digitali critici sulla base dei criteri di criticità di cui al presente regolamento e per specificare i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che possono essere utilizzati per dimostrare la conformità ai requisiti essenziali di cibersicurezza o a parti di essi stabiliti in allegato al presente regolamento. È opportuno delegare alla Commissione il potere di adottare atti per specificare il periodo minimo di assistenza per specifiche categorie di prodotti qualora i dati di sorveglianza del mercato suggeriscano periodi di assistenza inadeguati, nonché per specificare i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione delle notifiche riguardo alle vulnerabilità attivamente sfruttate. Inoltre, è opportuno delegare alla Commissione il potere di adottare atti per istituire programmi volontari di attestazione di sicurezza per valutare la conformità dei prodotti con elementi digitali che si qualificano come software liberi e open source a tutti o a determinati requisiti essenziali di cibersicurezza o ad altri obblighi stabiliti nel presente regolamento, nonché per specificare il contenuto minimo della dichiarazione di conformità UE e integrare gli elementi da includere nella documentazione tecnica. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([31]). In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati. Il potere di adottare atti delegati a norma del presente regolamento dovrebbe essere conferito alla Commissione per un periodo di cinque anni dalla data di entrata in vigore del presente regolamento. La Commissione dovrebbe elaborare una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere dovrebbe essere tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

(118) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione per specificare la descrizione tecnica delle categorie di prodotti con elementi digitali importanti in allegato al presente regolamento, specificare il formato e gli elementi della distinta base del software, specificare ulteriormente il formato e la procedura delle notifiche riguardo alle vulnerabilità attivamente sfruttate e agli incidenti gravi che incidono sulla sicurezza dei prodotti con elementi digitali presentate dai fabbricanti, stabilire specifiche comuni riguardanti i requisiti tecnici che forniscono i mezzi per conformarsi ai requisiti essenziali di cibersicurezza in allegato al presente regolamento, stabilire le specifiche tecniche per le etichette, i pittogrammi o qualsiasi altro marchio relativo alla sicurezza dei prodotti con elementi digitali, il periodo di sostegno e i meccanismi per promuoverne l'uso e sensibilizzare maggiormente il pubblico in merito alla sicurezza dei prodotti con elementi digitali, definire il modulo di documentazione semplificata rivolto alle esigenze delle microimprese e delle piccole imprese e decidere in merito a misure correttive o restrittive a livello dell'Unione in

([31]) GU L 123 del 12.5.2016, pag. 1.

circostanze eccezionali che giustifichino un intervento immediato per preservare il corretto funzionamento del mercato interno. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([32]).

(119) Al fine di garantire una cooperazione fiduciosa e costruttiva delle autorità di vigilanza del mercato a livello nazionale e dell'Unione, è opportuno che tutte le parti coinvolte nell'applicazione del presente regolamento rispettino la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti.

(120) Per garantire l'effettiva applicazione degli obblighi previsti dal presente regolamento, ogni autorità di vigilanza del mercato dovrebbe avere il potere di imporre o richiedere l'imposizione di sanzioni amministrative pecuniarie. È pertanto opportuno stabilire i livelli massimi delle sanzioni amministrative pecuniarie che devono essere previste negli ordinamenti nazionali in caso di mancato rispetto degli obblighi stabiliti dal presente regolamento. Nel decidere l'importo della sanzione amministrativa pecuniaria in ogni singolo caso si dovrebbe tenere conto di tutte le circostanze pertinenti della situazione specifica e, come minimo, di quelle esplicitamente stabilite nel presente regolamento, compresa l'eventualità che il fabbricante sia una microimpresa o una piccola o media impresa, compresa una start-up, e che le stesse o altre autorità di vigilanza del mercato abbiano già applicato sanzioni amministrative pecuniarie allo stesso operatore economico per una violazione analoga. Tali circostanze potrebbero costituire un'aggravante, nel caso in cui la violazione da parte dello stesso operatore economico si ripeta sul territorio di Stati membri diversi da quello in cui è già stata applicata una sanzione amministrativa pecuniaria, o un'attenuante, in quanto garantiscono che qualsiasi altra sanzione amministrativa pecuniaria presa in considerazione da un'altra autorità di vigilanza del mercato per lo stesso operatore economico o per lo stesso tipo di violazione tenga già conto, insieme ad altre circostanze specifiche pertinenti, di una sanzione e del suo importo imposti in altri Stati membri. In tutti questi casi la sanzione amministrativa pecuniaria cumulativa che le autorità di vigilanza del mercato di diversi Stati membri potrebbero applicare allo stesso operatore economico per lo stesso tipo di violazione dovrebbe garantire il rispetto del principio di proporzionalità. Dato che le sanzioni amministrative pecuniarie non si applicano alle microimprese o alle piccole imprese per il mancato rispetto del termine di 24 ore per la notifica di preallarme di vulnerabilità attivamente sfruttate o di incidenti gravi che hanno un impatto sulla sicurezza del prodotto con elementi digitali, né ai gestori di software open source per qualsiasi violazione del presente regolamento, e fatto salvo il principio secondo cui le sanzioni dovrebbero essere effettive, proporzionate e dissuasive, gli Stati membri non dovrebbero imporre a tali soggetti altri tipi di sanzioni a carattere pecuniario.

(121) Se le sanzioni amministrative pecuniarie sono inflitte a una persona che non è un'impresa, l'autorità competente dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie.

(122) Gli Stati membri dovrebbero esaminare, tenendo conto delle circostanze nazionali, la possibilità di utilizzare i proventi derivanti dalle sanzioni di cui al presente regolamento o il loro equivalente finanziario per sostenere politiche in materia di cibersicurezza e aumentare il livello di cibersicurezza nell'Unione, tra l'altro aumentando il numero di professionisti qualificati della cibersicurezza, rafforzando lo sviluppo di capacità per le microimprese e le piccole e medie imprese e migliorando la consapevolezza del pubblico in merito alle minacce informatiche.

(123) Nei suoi rapporti con i paesi terzi l'Unione si sforza di promuovere il commercio internazionale di prodotti soggetti a regolamentazione. Per agevolare gli scambi è possibile applicare un'ampia gamma di misure, tra cui diversi strumenti giuridici come gli accordi sul reciproco riconoscimento (ARR) bilaterali (intergovernativi) in materia di valutazione della conformità e marcatura dei prodotti soggetti a regolamentazione. Gli ARR sono conclusi tra l'Unione e i paesi terzi che presentano un livello comparabile di sviluppo tecnico e un approccio compatibile riguardo alla valutazione della conformità. Questi accordi si basano sulla reciproca accettazione di certificati, marchi di conformità e rapporti di prova rilasciati dagli organismi di valutazione della conformità di una parte conformemente alla normativa dell'altra parte. Attualmente sono in vigore ARR con diversi paesi terzi. Tali ARR sono conclusi in alcuni settori specifici, che possono variare da paese terzo a paese terzo. Al fine di agevolare ulteriormente gli scambi e riconoscendo che le catene di approvvigionamento dei prodotti con elementi digitali sono globali, l'Unione può concludere ARR relativi alla valutazione della conformità per i prodotti disciplinati dal presente regolamento, conformemente all'articolo 218 TFUE. Anche la cooperazione con i paesi terzi partner è importante per aumentare la ciberresilienza a livello globale, poiché a lungo termine ciò contribuirà a rafforzare il quadro della cibersicurezza sia all'interno che all'esterno dell'Unione.

([32]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

(124) I consumatori dovrebbero poter far valere i propri diritti in relazione agli obblighi incombenti agli operatori economici ai sensi del presente regolamento attraverso azioni rappresentative ai sensi della direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio ([33]). A tal fine, il presente regolamento dovrebbe prevedere che la direttiva (UE) 2020/1828 sia applicabile alle azioni rappresentative riguardanti violazioni del presente regolamento che ledono o possono ledere gli interessi collettivi dei consumatori. Occorre quindi modificare in tal senso l'allegato I di tale direttiva. Spetta agli Stati membri garantire che tali modifiche si riflettano nelle misure di recepimento adottate conformemente a tale direttiva, sebbene l'adozione di misure nazionali di recepimento a tale riguardo non sia una condizione per l'applicabilità di detta direttiva a tali azioni rappresentative. L'applicabilità di tale direttiva alle azioni rappresentative intentate nei confronti di violazioni di requisiti del presente regolamento da parte di operatori economici che ledono o potrebbero ledere gli interessi collettivi dei consumatori dovrebbe decorrere dall'11 dicembre 2027.

(125) È opportuno che la Commissione valuti e riesamini il presente regolamento periodicamente, in consultazione con i pertinenti portatori di interessi, in particolare al fine di valutare la necessità di modifiche alla luce dei cambiamenti delle condizioni sociali, politiche, tecnologiche o del mercato. Il presente regolamento faciliterà il rispetto degli obblighi di sicurezza della catena di approvvigionamento da parte dei soggetti che rientrano nell'ambito di applicazione del regolamento (UE) 2022/2554 e della direttiva (UE) 2022/2555 e utilizzano prodotti con elementi digitali. La Commissione dovrebbe valutare, nell'ambito di tale riesame periodico, gli effetti combinati del quadro dell'Unione in materia di cibersicurezza.

(126) Agli operatori economici dovrebbe essere concesso un periodo di tempo sufficiente per adeguarsi ai requisiti stabiliti nel presente regolamento. Il presente regolamento dovrebbe applicarsi a decorrere dall'11 dicembre 2027, ad eccezione degli obblighi di segnalazione delle vulnerabilità attivamente sfruttate e degli incidenti gravi aventi un impatto sulla sicurezza dei prodotti con elementi digitali, che dovrebbero applicarsi a decorrere dall'11 settembre 2026 e delle disposizioni sulla notifica degli organismi di valutazione della conformità che dovrebbero applicarsi a decorrere dall'11 giugno 2026.

(127) È importante fornire sostegno alle microimprese e alle piccole e medie imprese, comprese le start-up, nell'attuazione del presente regolamento e ridurre al minimo i rischi per l'attuazione derivanti dalla mancanza di conoscenze e competenze sul mercato nonché al fine di facilitare il rispetto, da parte dei fabbricanti, degli obblighi stabiliti nel presente regolamento. Il programma Europa digitale e altri programmi pertinenti dell'Unione forniscono sostegno finanziario e tecnico che consente a tali imprese di contribuire alla crescita dell'economia dell'Unione e al rafforzamento del livello comune di cibersicurezza nell'Unione. Anche il Centro europeo di competenza per la cibersicurezza, i centri nazionali di coordinamento e i poli europei dell'innovazione digitale istituiti dalla Commissione e dagli Stati membri a livello nazionale o dell'Unione potrebbero sostenere le imprese e le organizzazioni del settore pubblico e contribuire all'attuazione del presente regolamento. Nell'ambito delle rispettive missioni e ambiti di competenza, potrebbero fornire sostegno tecnico e scientifico alle microimprese e alle piccole e medie imprese, ad esempio per le attività di prova e le valutazioni della conformità da parte di terzi. Potrebbero inoltre promuovere la diffusione di strumenti per facilitare l'attuazione del presente regolamento.

(128) Inoltre, gli Stati membri dovrebbero prendere in considerazione azioni complementari volte a fornire orientamento e sostegno alle microimprese e alle piccole e medie imprese, come l'istituzione di spazi di sperimentazione normativa e canali appositi per la comunicazione. Al fine di rafforzare il livello di cibersicurezza nell'Unione, gli Stati membri possono anche prendere in considerazione la possibilità di fornire sostegno per sviluppare capacità e competenze relative alla cibersicurezza dei prodotti con elementi digitali, migliorare la ciberresilienza degli operatori economici, in particolare delle microimprese e delle piccole e medie imprese, e sensibilizzare l'opinione pubblica in merito alla cibersicurezza dei prodotti con elementi digitali.

(129) Poiché l'obiettivo del presente regolamento non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo degli effetti dell'azione in oggetto, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(130) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([34]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 9 novembre 2022 ([35]).

([33]) Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (GU L 409 del 4.12.2020, pag. 1).

([34]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

([35]) GU C 452 del 29.11.2022, pag. 23.

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

Il presente regolamento stabilisce:

a) norme per la messa a disposizione sul mercato di prodotti con elementi digitali per garantire la cibersicurezza di tali prodotti;

b) requisiti essenziali di cibersicurezza per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda la cibersicurezza;

c) requisiti essenziali di cibersicurezza per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti per garantire la cibersicurezza dei prodotti con elementi digitali durante il periodo in cui si prevede che i prodotti siano in uso e obblighi per gli operatori economici in relazione a tali processi;

d) norme sulla vigilanza del mercato, compreso il monitoraggio, e sull'applicazione delle norme e dei requisiti di cui al presente articolo.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete.

2. Il presente regolamento non si applica ai prodotti con elementi digitali a cui si applicano i seguenti atti giuridici dell'Unione:

a) regolamento (UE) 2017/745;

b) regolamento (UE) 2017/746;

c) regolamento (UE) 2019/2144.

3. Il presente regolamento non si applica ai prodotti con elementi digitali che sono stati certificati in conformità del regolamento (UE) 2018/1139.

4. Il presente regolamento non si applica all'equipaggiamento che rientra nell'ambito di applicazione della direttiva n. 2014/90/UE del Parlamento europeo e del Consiglio ([36]).

5. L'applicazione del presente regolamento ai prodotti con elementi digitali contemplati da altre norme dell'Unione, che stabiliscono requisiti che affrontano tutti o alcuni rischi contemplati dai requisiti essenziali di cibersicurezza di cui all'allegato I, può essere limitata o esclusa, qualora:

a) tale limitazione o esclusione sia coerente con il quadro normativo generale applicabile a tali prodotti; e

b) le norme settoriali conseguano lo stesso livello o un livello maggiore di protezione rispetto a quanto previsto dal presente regolamento.

Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 61 per integrare il presente regolamento specificando se tale limitazione o esclusione sia necessaria, i prodotti e le norme interessati, nonché l'ambito della limitazione, se pertinente.

([36]) Direttiva 2014/90/UE del Parlamento europeo e del Consiglio, del 23 luglio 2014, sull'equipaggiamento marittimo e che abroga la direttiva 96/98/CE del Consiglio (GU L 257 del 28.8.2014, pag. 146).

6. Il presente regolamento non si applica ai pezzi di ricambio messi a disposizione sul mercato per sostituire componenti identici in prodotti con elementi digitali e fabbricati secondo le stesse specifiche dei componenti che sono destinati a sostituire.

7. Il presente regolamento non si applica ai prodotti con elementi digitali sviluppati o modificati esclusivamente per scopi di sicurezza nazionale o di difesa o ai prodotti specificamente progettati per trattare informazioni classificate.

8. Gli obblighi definiti nel presente regolamento non comportano la comunicazione di informazioni la cui divulgazione sarebbe contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «prodotto con elementi digitali»: qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immesso sul mercato separatamente;

2) «elaborazione dati da remoto»: qualsiasi elaborazione dati a distanza per la quale il software è stato progettato e sviluppato dal fabbricante o sotto la sua responsabilità e la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni;

3) «cibersicurezza»: la cibersicurezza quale definita all'articolo 2, punto 1), del regolamento (UE) 2019/881;

4) «software»: la parte di un sistema di informazione elettronico costituita da un codice informatico;

5) «hardware»: un sistema di informazione elettronico fisico, o parti di esso, in grado di trattare, conservare o trasmettere dati digitali;

6) «componente»: il software o l'hardware destinato a essere integrato in un sistema di informazione elettronico;

7) «sistema di informazione elettronico»: un sistema, comprese le apparecchiature elettriche o elettroniche, in grado di trattare, conservare o trasmettere dati digitali;

8) «connessione logica»: una rappresentazione virtuale di una connessione dati realizzata attraverso un'interfaccia software;

9) «connessione fisica»: qualsiasi connessione tra sistemi di informazione elettronici o componenti realizzata con mezzi fisici, anche attraverso interfacce elettriche, ottiche o meccaniche, fili od onde radio;

10) «connessione indiretta»: una connessione a un dispositivo o a una rete che non avviene direttamente, ma piuttosto nell'ambito di un sistema più ampio che è direttamente collegabile a tale dispositivo o rete;

11) «terminale»: qualsiasi dispositivo connesso a una rete e che funge da punto di accesso a tale rete;

12) «operatore economico»: il fabbricante, il rappresentante autorizzato, l'importatore o il distributore, il fornitore di servizi di logistica o un'altra persona fisica o giuridica soggetta a obblighi in relazione alla fabbricazione di prodotti con elementi digitali o in relazione alla messa a disposizione sul mercato di prodotti con elementi digitali in conformità del presente regolamento;

13) «fabbricante»: una persona fisica o giuridica che sviluppa o fabbrica prodotti con elementi digitali o che fa progettare, sviluppare o fabbricare prodotti con elementi digitali e li commercializza con il proprio nome o marchio, a titolo oneroso, di monetizzazione o gratuito;

14) «gestore di software open source»: una persona giuridica, diversa dal fabbricante, che ha la finalità o l'obiettivo di fornire un sostegno sistematico e duraturo per lo sviluppo di prodotti specifici con elementi digitali, che si qualificano come software liberi e open source e destinati ad attività commerciali, e che garantisce la sostenibilità economica di tali prodotti;

15) «rappresentante autorizzato»: una persona fisica o giuridica stabilita nell'Unione che abbia ricevuto da un fabbricante un mandato scritto che la autorizza ad agire per suo conto in relazione a determinati compiti;

16) «importatore»: una persona fisica o giuridica stabilita nell'Unione che immette sul mercato un prodotto con elementi digitali recante il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione;

17) «distributore»: una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fabbricante o dall'importatore, che mette a disposizione un prodotto con elementi digitali sul mercato dell'Unione senza modificarne le proprietà;

18) «consumatore»: una persona fisica che agisce per scopi estranei alla propria attività commerciale, imprenditoriale, artigianale o professionale;

19) «microimprese», «piccole imprese» e «medie imprese», rispettivamente: le micro imprese, le piccole imprese e le medie imprese quali definite nell'allegato alla raccomandazione 2003/361/CE;

20) «periodo di assistenza»: il periodo durante il quale un fabbricante garantisce che le vulnerabilità di un prodotto con elementi digitali siano gestite in modo efficace e conformemente ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte II;

21) «immissione sul mercato»: la prima messa a disposizione di un prodotto con elementi digitali sul mercato dell'Unione;

22) «messa a disposizione sul mercato»: la fornitura, a titolo oneroso o gratuito, di un prodotto con elementi digitali perché sia distribuito o usato sul mercato dell'Unione nel corso di un'attività commerciale;

23) «finalità prevista»: l'uso di un prodotto con elementi digitali previsto dal fabbricante, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fabbricante nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica;

24) «uso ragionevolmente prevedibile»: un uso che non corrisponde necessariamente alla finalità prevista dal fabbricante nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica, ma che è probabile possa derivare da un comportamento umano o da operazioni o interazioni tecniche ragionevolmente prevedibili;

25) «uso improprio ragionevolmente prevedibile»: l'uso di un prodotto con elementi digitali in un modo non conforme alla sua finalità prevista, ma che può derivare da un comportamento umano o da un'interazione con altri sistemi ragionevolmente prevedibili;

26) «autorità di notifica»: l'autorità nazionale responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio;

27) «valutazione della conformità»: il processo atto a verificare il rispetto dei requisiti essenziali di cibersicurezza di cui all'allegato I;

28) «organismo di valutazione della conformità»: organismo di valutazione della conformità quale definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008.

29) «organismo notificato»: un organismo di valutazione della conformità designato in conformità del presente regolamento e di altre pertinenti normative di armonizzazione dell'Unione;

30) «modifica sostanziale»: una modifica del prodotto con elementi digitali a seguito della sua immissione sul mercato che incide sulla conformità del prodotto con elementi digitali ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, o che comporta una modifica della finalità prevista per la quale il prodotto con elementi digitali è stato valutato;

31) «marcatura CE»: una marcatura mediante cui un fabbricante indica che un prodotto con elementi digitali e i processi messi in atto dal fabbricante sono conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I e ad altre normative di armonizzazione applicabili dell'Unione e che ne prevedono l'apposizione;

32) «normativa di armonizzazione dell'Unione»: la normativa dell'Unione elencata nell'allegato I del regolamento (UE) 2019/1020 e qualsiasi altra normativa dell'Unione che armonizza le condizioni di commercializzazione dei prodotti cui si applica tale regolamento;

33) «autorità di vigilanza del mercato»: un'autorità di vigilanza del mercato quale definita all'articolo 3, punto 4), del regolamento (UE) 2019/1020;

34) «norma internazionale»: una norma internazionale quale definita all'articolo 2, punto 1), lettera a), del regolamento (UE) n. 1025/2012;

35) «norma europea»: una norma europea quale definita all'articolo 2, punto 1), lettera b), del regolamento (UE) n. 1025/2012;

36) «norma armonizzata»: una norma armonizzata, quale definita all'articolo 2, punto 1), lettera c), del regolamento (UE) n. 1025/2012;

37) «rischio di cibersicurezza»: la potenziale perdita o perturbazione causata da un incidente da esprimersi come combinazione dell'entità di tale perdita o perturbazione e della probabilità che si verifichi l'incidente;

38) «rischio di cibersicurezza significativo»: un rischio di cibersicurezza che, in base alle sue caratteristiche tecniche, si può presumere abbia una probabilità elevata di provocare un incidente che potrebbe avere un impatto negativo grave, causando anche notevoli perdite o perturbazioni materiali o non materiali;

39) «distinta base del software»: un registro formale contenente i dettagli e le relazioni della catena di approvvigionamento dei componenti inclusi negli elementi software di un prodotto con elementi digitali;

40) «vulnerabilità»: un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica;

41) «vulnerabilità sfruttabile»: una vulnerabilità che può essere utilizzata efficacemente da un avversario in condizioni operative pratiche;

42) «vulnerabilità attivamente sfruttata»: una vulnerabilità per la quale esistono prove attendibili che un soggetto malintenzionato l'ha sfruttata in un sistema senza l'autorizzazione del proprietario del sistema;

43) «incidente»: un incidente quale definito all'articolo 6, punto 6), della direttiva (UE) 2022/2555;

44) «incidente che ha un impatto sulla sicurezza del prodotto con elementi digitali»: un incidente che incide negativamente o è in grado di incidere negativamente sulla capacità di un prodotto con elementi digitali di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati o funzioni;

45) «quasi incidente»: un quasi incidente quale definito all'articolo 6, punto 5), della direttiva (UE) 2022/2555;

46) «minaccia informatica»: una minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881;

47) «dati personali»: i dati personali ai sensi dell'articolo 4, punto 1), del regolamento (UE) 2016/679;

48) «software libero e open source»: un software il cui codice sorgente è condiviso apertamente e che è messo a disposizione nell'ambito di una licenza gratuita e open source che prevede tutti i diritti per renderlo liberamente accessibile, utilizzabile, modificabile e ridistribuibile;

49) «richiamo»: un richiamo ai sensi dell'articolo 3, punto 22), del regolamento (UE) 2019/1020;

50) «ritiro»: un ritiro quale definito all'articolo 3, punto 23), del regolamento (UE) 2019/1020;

51) «CSIRT designato come coordinatore»: un CSIRT designato come coordinatore a norma dell'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555.

Articolo 4

Libera circolazione

1. Gli Stati membri non impediscono, per gli aspetti disciplinati dal presente regolamento, la messa a disposizione sul mercato di prodotti con elementi digitali che sono conformi al presente regolamento.

2. In occasione di fiere, mostre e dimostrazioni o eventi analoghi, gli Stati membri non impediscono la presentazione e l'uso di un prodotto con elementi digitali non conforme al presente regolamento, compresi i suoi prototipi, a condizione che il prodotto presenti un'indicazione visibile che specifichi chiaramente che esso non è conforme al presente regolamento e che non deve essere messo a disposizione sul mercato finché non lo sarà.

3. Gli Stati membri non impediscono la messa a disposizione sul mercato di un software non finito non conforme al presente regolamento, a condizione che il software sia reso disponibile solo per un periodo limitato necessario ai fini di prova e con un'indicazione visibile che specifichi chiaramente che esso non è conforme al presente regolamento e che non sarà disponibile sul mercato per fini diversi dalla prova.

4. Il paragrafo 3 non si applica ai componenti di sicurezza di cui alla normativa di armonizzazione dell'Unione diversa dal presente regolamento.

Articolo 5

Acquisto o utilizzo di prodotti con elementi digitali

1. Il presente regolamento non osta a che gli Stati membri assoggettino i prodotti con elementi digitali a requisiti di cibersicurezza supplementari per l'acquisto o l'utilizzo di tali prodotti per fini specifici, anche nel caso in cui tali prodotti siano acquistati o utilizzati per scopi di sicurezza nazionale o di difesa, purché tali requisiti siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione e siano necessari e proporzionati al conseguimento di tali scopi.

2. Fatte salve le direttive 2014/24/UE e 2014/25/UE, in caso di acquisto di prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento, gli Stati membri garantiscono che la conformità ai requisiti essenziali di cibersicurezza di cui all'allegato I del presente regolamento, compresa la capacità dei fabbricanti di gestire efficacemente le vulnerabilità, sia presa in considerazione nella procedura di appalto.

Articolo 6

Requisiti per i prodotti con elementi digitali

I prodotti con elementi digitali sono messi a disposizione sul mercato soltanto se:

a) soddisfano i requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, a condizione che siano correttamente installati, siano oggetto di un'adeguata manutenzione e siano utilizzati conformemente alla loro finalità prevista o in condizioni ragionevolmente prevedibili e, se applicabile, siano stati installati i necessari aggiornamenti di sicurezza, e

b) i processi messi in atto dal fabbricante sono conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte II.

Articolo 7

Prodotti con elementi digitali importanti

1. I prodotti con elementi digitali che hanno la funzionalità principale di una categoria di prodotti di cui all'allegato III sono considerati prodotti con elementi digitali importanti e sono soggetti alle procedure di valutazione della conformità di cui all'articolo 32, paragrafi 2 e 3. L'integrazione di un prodotto con elementi digitali che ha la funzionalità principale di una categoria di prodotti di cui all'allegato III non rende di per sé il prodotto in cui è integrato assoggettato alle procedure di valutazione della conformità di cui all'articolo 32, paragrafi 2 e 3.

2. Le categorie di prodotti con elementi digitali di cui al paragrafo 1 del presente articolo, suddivise nelle classi I e II di cui all'allegato III, soddisfano almeno uno dei criteri seguenti:

a) il prodotto con elementi digitali svolge principalmente funzioni essenziali per la cibersicurezza di altri prodotti, reti o servizi, tra cui la sicurezza dell'autenticazione e dell'accesso, la prevenzione e il rilevamento delle intrusioni, la sicurezza dei terminali o la protezione della rete;

b) il prodotto con elementi digitali svolge una funzione che comporta un rischio significativo di avere effetti negativi in ragione della sua intensità e capacità di perturbare, controllare o danneggiare un gran numero di altri prodotti o la salute, la sicurezza o l'incolumità dei suoi utenti attraverso la manipolazione diretta, come una funzione centrale di sistema, compresi la gestione della rete, il controllo di configurazione, la virtualizzazione o il trattamento dei dati personali.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 61 al fine di modificare l'allegato III, includendo nell'elenco una nuova categoria all'interno di ciascuna classe di categorie di prodotti con elementi digitali e specificandone la definizione, spostando una categoria di prodotti da una classe all'altra o eliminandone una categoria esistente. Nel valutare la necessità di modificare l'elenco di cui all'allegato III, la Commissione tiene conto delle funzionalità relative alla cibersicurezza o della funzione e del livello di rischio di cibersicurezza posto dai prodotti con elementi digitali come stabilito dai criteri di cui al paragrafo 2 del presente articolo.

Gli atti delegati di cui al primo comma del presente paragrafo prevedono, se del caso, un periodo di transizione minimo di 12 mesi, in particolare qualora una nuova categoria di prodotti con elementi digitali importanti sia aggiunta alla classe I o II o sia spostata dalla classe I alla classe II di cui all'allegato III, prima che inizino ad applicarsi le pertinenti procedure di valutazione della conformità di cui all'articolo 32, paragrafi 2 e 3, a meno che un periodo di transizione più breve non sia giustificato da imperativi motivi di urgenza.

4. Entro l'11 dicembre 2025 la Commissione adotta un atto di esecuzione che specifica la descrizione tecnica delle categorie di prodotti con elementi digitali delle classi I e II di cui all'allegato III e la descrizione tecnica delle categorie di prodotti con elementi digitali di cui all'allegato IV. Tale atto di esecuzione è adottato conformemente alla procedura d'esame di cui all'articolo 62, paragrafo 2.

Articolo 8

Prodotti con elementi digitali critici

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 61 al fine di integrare il presente regolamento per determinare quali prodotti con elementi digitali aventi la funzionalità principale di una categoria di prodotti di cui all'allegato IV del presente regolamento debbano essere tenuti a ottenere un certificato europeo di cibersicurezza a un livello di affidabilità almeno «sostanziale» nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma del regolamento (UE) 2019/881, al fine di dimostrare la conformità ai requisiti essenziali di cibersicurezza di cui all'allegato I del presente regolamento o parti di essi, a condizione che un sistema europeo di certificazione della cibersicurezza che copra tali categorie di prodotti con elementi digitali sia stato adottato a norma del regolamento (UE) 2019/881 e sia a disposizione dei fabbricanti. Tali atti delegati specificano il livello di affidabilità richiesto che è proporzionato al livello di rischio di cibersicurezza associato ai prodotti con elementi digitali e tengono conto della loro finalità prevista, compresa la dipendenza critica da essi da parte dei soggetti essenziali di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555.

Prima di adottare tali atti delegati, la Commissione effettua una valutazione del potenziale impatto sul mercato delle misure previste e procede a consultazioni con i portatori di interessi pertinenti, compreso il gruppo europeo per la certificazione della cibersicurezza istituto a norma del regolamento (UE) 2019/881. La valutazione tiene conto della preparazione e del livello di capacità degli Stati membri per l'attuazione del pertinente sistema europeo di certificazione della cibersicurezza. Qualora non siano stati adottati gli atti delegati di cui al primo comma del presente paragrafo, i prodotti con elementi digitali che hanno la funzionalità principale di una categoria di prodotti di cui all'allegato IV sono soggetti alle procedure di valutazione della conformità di cui all'articolo 32, paragrafo 3.

Gli atti delegati di cui al primo comma prevedono un periodo di transizione minimo di sei mesi, a meno che un periodo di transizione più breve non sia giustificato da imperativi motivi di urgenza.

2. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 61 per modificare l'allegato IV aggiungendo o ritirando categorie di prodotti con elementi digitali critici. Nel determinare tali categorie di prodotti con elementi digitali critici e il livello di affidabilità richiesto, conformemente al paragrafo 1 del presente articolo, la Commissione tiene conto dei criteri di cui all'articolo 7, paragrafo 2, e garantisce che le categorie di prodotti con elementi digitali soddisfano almeno uno dei criteri seguenti:

a) vi è una dipendenza critica dei soggetti essenziali di cui all'articolo 3 della direttiva (UE) 2022/2555 dalla categoria di prodotti con elementi digitali;

b) gli incidenti e le vulnerabilità sfruttate riguardanti la categoria di prodotti con elementi digitali potrebbero causare gravi perturbazioni delle catene di approvvigionamento critiche in tutto il mercato interno.

Prima di adottare tali atti delegati, la Commissione effettua una valutazione del tipo di cui al paragrafo 1.

Gli atti delegati di cui al primo comma prevedono un periodo di transizione minimo di sei mesi, a meno che un periodo di transizione più breve non sia giustificato da imperativi motivi di urgenza.

Articolo 9

Consultazione dei portatori di interessi

1. Nell'elaborare misure per l'attuazione del presente regolamento, la Commissione consulta e tiene conto dei pareri dei pertinenti portatori di interessi, quali le autorità competenti degli Stati membri, le imprese del settore privato, comprese le microimprese e le piccole e medie imprese, la comunità del software open source, le associazioni dei consumatori, il mondo accademico e le agenzie e gli organismi pertinenti dell'Unione, nonché i gruppi di esperti istituiti a livello dell'Unione. In particolare, la Commissione consulta e raccoglie i pareri di tali portatori di interessi in modo strutturato, se del caso, quando:

a) elabora gli orientamenti di cui all'articolo 26;

b) prepara le descrizioni tecniche delle categorie di prodotti di cui all'allegato III conformemente all'articolo 7, paragrafo 4, valuta la necessità di potenziali aggiornamenti dell'elenco delle categorie di prodotti conformemente all'articolo 7, paragrafo 3, e all'articolo 8, paragrafo 2, o effettua la valutazione del potenziale impatto sul mercato di cui all'articolo 8, paragrafo 1, fatto salvo l'articolo 61;

c) svolge lavori preparatori per la valutazione e il riesame del presente regolamento.

2. La Commissione organizza periodicamente sessioni di consultazione e informazione, almeno una volta all'anno, per raccogliere i pareri delle parti interessate di cui al paragrafo 1 sull'attuazione del presente regolamento.

Articolo 10

Migliorare le competenze in un ambiente digitale ciberresiliente

Ai fini del presente regolamento e per rispondere alle esigenze dei professionisti a sostegno dell'attuazione del presente regolamento, gli Stati membri, se del caso, con il sostegno della Commissione, del Centro europeo di competenza per la cibersicurezza e dell'ENISA, nel pieno rispetto della responsabilità degli Stati membri nel settore dell'istruzione, promuovono misure e strategie volte a:

a) sviluppare competenze in materia di cibersicurezza e creare strumenti organizzativi e tecnologici per garantire una disponibilità sufficiente di professionisti qualificati al fine di sostenere le attività delle autorità di vigilanza del mercato e degli organismi di valutazione della conformità;

b) ad aumentare la collaborazione tra il settore privato, gli operatori economici, anche attraverso la riqualificazione o il miglioramento delle competenze dei dipendenti dei fabbricanti, i consumatori, gli erogatori di istruzione e formazione e le pubbliche amministrazioni, ampliando le possibilità per i giovani di accedere a posti di lavoro nel settore della cibersicurezza.

Articolo 11

Sicurezza generale dei prodotti

In deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento (UE) 2023/988, il capo III, sezione 1, i capi V e VII e i capi da IX a XI di tale regolamento si applicano ai prodotti con elementi digitali per quanto riguarda gli aspetti e i rischi o le categorie di rischio non contemplati dal presente regolamento qualora tali prodotti non siano soggetti a requisiti specifici di sicurezza imposti da altra «normativa di armonizzazione dell'Unione» ai sensi dell'articolo 3, punto 27), del regolamento (UE) 2023/988.

Articolo 12

Sistemi di IA ad alto rischio

1. Fatti salvi i requisiti relativi all'accuratezza e alla robustezza di cui all'articolo 15 del regolamento (UE) 2024/1689, i prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento e sono classificati come sistemi di IA ad alto rischio ai sensi dell'articolo 6 di tale regolamento sono considerati conformi ai requisiti relativi alla cibersicurezza di cui all'articolo 15 di tale regolamento qualora:

a) tali prodotti soddisfino i requisiti essenziali di cibersicurezza di cui all'allegato I, parte I;

b) i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte II; e

c) il conseguimento del livello di protezione della cibersicurezza richiesta a norma dell'articolo 15 del regolamento (UE) 2024/1689 sia dimostrato nella dichiarazione di conformità UE rilasciata a norma del presente regolamento.

2. Per quanto riguarda i prodotti con elementi digitali e i requisiti di cibersicurezza di cui al paragrafo 1, del presente articolo si applica la pertinente procedura di valutazione della conformità prevista dall'articolo 43 del regolamento (UE) 2024/1689. Ai fini di tale valutazione, gli organismi notificati che sono competenti a controllare la conformità dei sistemi di IA ad alto rischio a norma del regolamento (UE) 2024/1689 sono anche competenti a controllare la conformità dei sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del presente regolamento ai requisiti di cui all'allegato I del presente regolamento, a condizione che la conformità di tali organismi notificati ai requisiti di cui all'articolo 39 del presente regolamento sia stata valutata nel contesto della procedura di notifica di cui al regolamento (UE) 2024/1689.

3. In deroga al paragrafo 2 del presente articolo, i prodotti con elementi digitali importanti di cui all'allegato III del presente regolamento che sono soggetti alle procedure di valutazione della conformità di cui all'articolo 32, paragrafo 2, lettere a) e b), e paragrafo 3, del presente regolamento e i prodotti con elementi digitali critici elencati nell'allegato IV del presente regolamento che sono tenuti a ottenere un certificato europeo di cibersicurezza ai sensi dell'articolo 8, paragrafo 1, del presente regolamento o, in assenza di tale certificato, sono soggetti alle procedure di valutazione della conformità di cui all'articolo 32, paragrafo 3, del presente regolamento, e che sono anche classificati come sistemi di IA ad alto rischio ai sensi dell'articolo 6 del regolamento (UE) 2024/1689 e ai quali si applica la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI del regolamento (UE) 2024/1689, sono soggetti alle procedure di valutazione della conformità previste dal presente regolamento per quanto riguarda i requisiti essenziali di cibersicurezza stabiliti nel presente regolamento.

4. I fabbricanti di prodotti con elementi digitali di cui al paragrafo 1 del presente regolamento possono partecipare agli spazi di sperimentazione normativa per l'IA di cui all'articolo 57 del regolamento (UE) 2024/1689.

CAPO II

OBBLIGHI DEGLI OPERATORI ECONOMICI E DISPOSIZIONI IN MATERIA DI SOFTWARE LIBERI E OPEN SOurce

Articolo 13

Obblighi dei fabbricanti

1. All'atto dell'immissione sul mercato di un prodotto con elementi digitali, i fabbricanti assicurano che esso sia stato progettato, sviluppato e prodotto conformemente ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I.

2. Ai fini della conformità al paragrafo 1, i fabbricanti effettuano una valutazione dei rischi di cibersicurezza associati a un prodotto con elementi digitali e tengono conto dei risultati di tale valutazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto con elementi digitali, allo scopo di ridurre al minimo i rischi di cibersicurezza, prevenire gli incidenti e ridurne al minimo il loro impatto, anche in relazione alla salute e alla sicurezza degli utilizzatori.

3. La valutazione dei rischi di cibersicurezza è documentata e aggiornata, se del caso, durante un periodo di assistenza da determinare conformemente al paragrafo 8 del presente articolo. Tale valutazione comprende almeno un'analisi dei rischi di cibersicurezza basata sulla finalità prevista e sull'uso ragionevolmente prevedibile del prodotto con elementi digitali, nonché sulle sue condizioni d'uso, quali l'ambiente operativo o gli attivi da proteggere, tenendo conto della durata di utilizzo del prodotto prevista. La valutazione dei rischi di cibersicurezza indica se, ed eventualmente in che modo, i requisiti di sicurezza di cui all'allegato I, parte I, punto 2, sono applicabili al pertinente prodotto con elementi digitali e le modalità di attuazione di tali requisiti sulla base della valutazione dei rischi di cibersicurezza. Indica inoltre le modalità con cui il fabbricante intende applicare l'allegato I, parte I, punto 1, e i requisiti di gestione delle vulnerabilità di cui all'allegato I, parte II.

4. All'atto dell'immissione sul mercato di un prodotto con elementi digitali, il fabbricante include la valutazione dei rischi di cibersicurezza di cui al paragrafo 3 del presente articolo nella documentazione tecnica richiesta a norma dell'articolo 31 e dell'allegato VII. Per i prodotti con elementi digitali di cui all'articolo 12, che sono soggetti anche ad altri atti giuridici dell'Unione, la valutazione dei rischi di cibersicurezza può far parte della valutazione dei rischi prevista da tali atti giuridici dell'Unione. Se alcuni requisiti essenziali di cibersicurezza non sono applicabili al prodotto con elementi digitali, il fabbricante fornisce una chiara giustificazione in tal senso nella suddetta documentazione tecnica.

5. Ai fini dell'adempimento dell'obbligo di cui al paragrafo 1, i fabbricanti esercitano la dovuta diligenza quando integrano componenti provenienti da terzi affinché tali componenti non compromettano la cibersicurezza del prodotto con elementi digitali, anche quando integrano componenti di software liberi e open source che non sono stati messi a disposizione sul mercato nel corso di un'attività commerciale.

6. Quando è individuata una vulnerabilità in un componente, compreso un componente open source, integrato nel prodotto con elementi digitali, i fabbricanti la segnalano alla persona o al soggetto che si occupa della fabbricazione o della manutenzione del componente e affrontano e correggono la vulnerabilità conformemente ai requisiti di gestione delle vulnerabilità di cui all'allegato I, parte II. Qualora abbiano sviluppato una modifica del software o dell'hardware per affrontare la vulnerabilità di tale componente, i fabbricanti condividono il codice o la documentazione pertinenti con la persona o il soggetto che si occupa della fabbricazione o della manutenzione del componente, se del caso in un formato leggibile da un dispositivo automatico.

7. I fabbricanti documentano sistematicamente, in modo proporzionato alla natura e ai rischi di cibersicurezza, gli aspetti pertinenti di cibersicurezza relativi al prodotto con elementi digitali, comprese le vulnerabilità di cui vengono a conoscenza e qualsiasi informazione pertinente fornita da terzi e, se del caso, aggiornano la valutazione dei rischi di cibersicurezza del prodotto.

8. All'atto dell'immissione sul mercato di un prodotto con elementi digitali e per la durata del periodo di assistenza, i fabbricanti garantiscono che le vulnerabilità di tale prodotto, compresi i suoi componenti, siano gestite in modo efficace e in conformità dei requisiti essenziali di cibersicurezza di cui all'allegato I, parte II.

I fabbricanti determinano il periodo di assistenza in modo che rifletta la durata di utilizzo prevista del prodotto, tenendo conto, in particolare, delle ragionevoli aspettative degli utilizzatori, della natura del prodotto, compresa la sua finalità prevista, nonché del pertinente diritto dell'Unione che determina la durata di vita dei prodotti con elementi digitali. Nel determinare il periodo di assistenza, i fabbricanti possono tenere conto anche dei periodi di assistenza dei prodotti con elementi digitali che offrono funzionalità analoghe immessi sul mercato da altri fabbricanti, della disponibilità dell'ambiente operativo, dei periodi di assistenza dei componenti integrati che forniscono funzioni essenziali e che provengono da terzi, nonché degli orientamenti pertinenti forniti dall'apposito gruppo di cooperazione amministrativa (ADCO) istituito a norma dell'articolo 52, paragrafo 15, e dalla Commissione. Le questioni da prendere in considerazione per determinare il periodo di assistenza sono prese in considerazione in modo da garantire la proporzionalità.

Fatto salvo il secondo comma, il periodo di assistenza è di almeno cinque anni. Se si prevede che il prodotto con elementi digitali sarà utilizzato per meno di cinque anni, il periodo di assistenza corrisponde alla durata di utilizzo prevista.

Tenendo conto delle raccomandazioni dell'ADCO di cui all'articolo 52, paragrafo 16, la Commissione può adottare atti delegati conformemente all'articolo 61 al fine di integrare il presente regolamento specificando il periodo minimo di assistenza per determinate categorie di prodotti qualora i dati di vigilanza del mercato suggeriscano l'inadeguatezza dei periodi di assistenza.

I fabbricanti includono nella documentazione tecnica di cui all'allegato VII le informazioni prese in considerazione per determinare il periodo di assistenza di un prodotto con elementi digitali.

I fabbricanti dispongono di politiche e procedure adeguate, comprese politiche di divulgazione coordinata delle vulnerabilità, di cui all'allegato I, parte II, punto 5, per trattare e correggere potenziali vulnerabilità del prodotto con elementi digitali segnalate da fonti interne o esterne.

9. I fabbricanti garantiscono che ciascun aggiornamento di sicurezza di cui all'allegato I, parte II, punto 8, che è stato messo a disposizione degli utilizzatori durante il periodo di assistenza, rimanga disponibile dopo il rilascio per un minimo di dieci anni o per il restante periodo di assistenza, se quest'ultimo è superiore.

10. Il fabbricante che abbia immesso sul mercato versioni successive sostanzialmente modificate di un software può garantire la conformità al requisito essenziale di cibersicurezza di cui all'allegato I, parte II, punto 2, solo per l'ultima versione immessa sul mercato, a condizione che gli utilizzatori delle versioni precedentemente immesse sul mercato abbiano accesso gratuito all'ultima versione immessa sul mercato e non debbano sostenere costi aggiuntivi per adeguare l'ambiente hardware e software in cui utilizzano la versione originale del prodotto.

11. I fabbricanti possono tenere archivi pubblici di software per migliorare l'accesso degli utilizzatori alle versioni precedenti. In questi casi, gli utilizzatori sono informati in modo chiaro e facilmente accessibile dei rischi associati all'uso di software privi di assistenza.

12. Prima di immettere un prodotto con elementi digitali sul mercato, i fabbricanti redigono la documentazione tecnica di cui all'articolo 31.

Essi seguono o fanno eseguire le procedure di valutazione della conformità prescelte di cui all'articolo 32.

Se tale procedura di valutazione della conformità dimostra la conformità del prodotto con elementi digitali ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e dei processi messi in atto dal fabbricante ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte II, i fabbricanti redigono la dichiarazione di conformità UE conformemente all'articolo 28 e appongono la marcatura CE conformemente all'articolo 30.

13. I fabbricanti tengono la documentazione tecnica e la dichiarazione di conformità UE a disposizione delle autorità di vigilanza del mercato per un periodo di almeno dieci anni dalla data di immissione sul mercato del prodotto con elementi digitali o per il periodo di assistenza, se quest'ultimo è superiore.

14. I fabbricanti si assicurano che siano predisposte le procedure necessarie affinché i prodotti con elementi digitali fabbricati nell'ambito di una produzione in serie rimangano conformi al presente regolamento. I fabbricanti tengono adeguatamente conto delle modifiche del processo di sviluppo e di produzione o della progettazione o delle caratteristiche del prodotto con elementi digitali, nonché delle modifiche delle norme armonizzate, dei sistemi europei di certificazione della cibersicurezza o delle specifiche comuni di cui all'articolo 27 con riferimento alle quali è dichiarata la conformità del prodotto con elementi digitali o mediante applicazione delle quali tale conformità è verificata.

15. I fabbricanti garantiscono che i loro prodotti con elementi digitali rechino un numero di tipo, di lotto o di serie o qualsiasi altro elemento che ne consenta l'identificazione, oppure, qualora ciò non sia possibile, che tali informazioni siano fornite sull'imballaggio o in un documento di accompagnamento del prodotto con elementi digitali.

16. I fabbricanti indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato, l'indirizzo postale, l'indirizzo di posta elettronica o altri dati di contatto digitale nonché, se disponibile, il sito web presso cui possono essere contattati, sul prodotto con elementi digitali, sull'imballaggio o in un documento di accompagnamento del prodotto con elementi digitali. Tali informazioni sono incluse anche nelle informazioni e nelle istruzioni per l'utilizzatore di cui all'allegato II. I dati di recapito sono redatti in una lingua facilmente comprensibile dagli utilizzatori e dalle autorità di vigilanza del mercato.

17. Ai fini del presente regolamento, i fabbricanti designano un punto di contatto unico che consenta agli utilizzatori di comunicare direttamente e rapidamente con loro, anche per facilitare la segnalazione di vulnerabilità del prodotto con elementi digitali.

I fabbricanti garantiscono che il punto di contatto unico sia facilmente identificabile dagli utilizzatori. Essi includono inoltre il punto di contatto unico nelle informazioni e istruzioni per l'utilizzatore di cui all'allegato II.

Il punto di contatto unico consente agli utilizzatori di scegliere i mezzi di comunicazione preferiti, senza limitarli agli strumenti automatizzati.

18. I fabbricanti provvedono affinché i prodotti con elementi digitali siano accompagnati dalle informazioni e dalle istruzioni per l'utilizzatore di cui all'allegato II in forma cartacea o elettronica. Tali informazioni e istruzioni sono fornite in una lingua facilmente comprensibile dagli utilizzatori e dalle autorità di vigilanza del mercato. Sono chiare, comprensibili, intelligibili e leggibili. Consentono un'installazione, un funzionamento e un utilizzo sicuri dei prodotti con elementi digitali. I fabbricanti mantengono a disposizione degli utilizzatori e delle autorità di vigilanza del mercato le informazioni e istruzioni per l'utilizzatore di cui all'allegato II per un periodo di almeno dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per il periodo di assistenza, se quest'ultimo è superiore. Qualora tali informazioni e istruzioni siano fornite online, i fabbricanti garantiscono che siano accessibili, di facile uso e disponibili online per un periodo di almeno dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per il periodo di assistenza, se quest'ultimo è superiore.

19. I fabbricanti garantiscono che la data finale del periodo di assistenza di cui al paragrafo 8, comprendente almeno il mese e l'anno, sia specificata in modo chiaro e comprensibile al momento dell'acquisto in modo facilmente accessibile e, se del caso, sul prodotto con elementi digitali, sul suo imballaggio o con mezzi digitali.

Ove tecnicamente fattibile alla luce della natura del prodotto con elementi digitali, i fabbricanti inviano una notifica agli utilizzatori per informarli che il loro prodotto con elementi digitali ha raggiunto la fine del periodo di assistenza.

20. I fabbricanti forniscono una copia della dichiarazione di conformità UE o una dichiarazione di conformità UE semplificata con il prodotto con elementi digitali. Se è fornita una dichiarazione di conformità UE semplificata, questa contiene l'esatto indirizzo Internet dove è possibile accedere alla dichiarazione di conformità UE completa.

21. A partire dall'immissione sul mercato e per la durata del periodo di assistenza, i fabbricanti che hanno la certezza o motivo di credere che il prodotto con elementi digitali o i processi messi in atto dal fabbricante non siano conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I adottano immediatamente le misure correttive necessarie per rendere conformi il prodotto con elementi digitali o i processi del fabbricante oppure, a seconda dei casi, per ritirare o richiamare il prodotto.

22. I fabbricanti, su richiesta motivata di un'autorità di vigilanza del mercato, forniscono a tale autorità, in una lingua che può essere facilmente compresa da quest'ultima, tutte le informazioni e la documentazione, in formato cartaceo o elettronico, necessarie a dimostrare la conformità del prodotto con elementi digitali e dei processi messi in atto dal fabbricante ai requisiti essenziali di cibersicurezza di cui all'allegato I. I fabbricanti cooperano con tale autorità, su richiesta di quest'ultima, in merito a qualsiasi misura adottata per eliminare i rischi di cibersicurezza presentati dal prodotto con elementi digitali che hanno immesso sul mercato.

23. Il fabbricante che cessa l'attività e di conseguenza non è in grado di conformarsi al presente regolamento informa, prima che la cessazione dell'attività abbia effetto, le autorità di vigilanza del mercato competenti, nonché, con ogni mezzo disponibile e nella misura del possibile, gli utilizzatori dei prodotti pertinenti con elementi digitali interessati immessi sul mercato, dell'imminente cessazione dell'attività.

24. La Commissione può, mediante atti di esecuzione che tengano conto delle norme e delle migliori pratiche europee o internazionali, specificare il formato e gli elementi della distinta base del software di cui all'allegato I, parte II, punto 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

25. Al fine di valutare la dipendenza degli Stati membri e dell'Unione nel suo complesso dai componenti software e, in particolare, dai componenti che si qualificano come software liberi e open source, l'ADCO può decidere di condurre una valutazione della dipendenza a livello dell'Unione per determinate categorie di prodotti con elementi digitali. A tal fine, le autorità di vigilanza del mercato possono chiedere ai fabbricanti di tali categorie di prodotti con elementi digitali di fornire le distinte base del software pertinenti di cui all'allegato I, parte II, punto 1. Sulla base di tali informazioni, le autorità di vigilanza del mercato possono fornire all'ADCO informazioni anonimizzate e aggregate sulle dipendenze in materia di software. L'ADCO presenta una relazione sui risultati della valutazione delle dipendenze al gruppo di cooperazione istituito a norma dell'articolo 14 della direttiva (UE) 2022/2555.

Articolo 14

Obblighi di segnalazione dei fabbricanti

1. Un fabbricante notifica simultaneamente al CSIRT designato come coordinatore, conformemente al paragrafo 7 del presente articolo, e all'ENISA, qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali di cui viene a conoscenza. Il fabbricante notifica tale vulnerabilità attivamente sfruttata tramite la piattaforma unica di segnalazione istituita a norma dell'articolo 16.

2. Ai fini della notifica di cui al paragrafo 1, il fabbricante presenta:

a) una notifica di preallarme di una vulnerabilità attivamente sfruttata, senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui il fabbricante ne è venuto a conoscenza, che indichi, se del caso, gli Stati membri sul cui territorio il fabbricante sia al corrente del fatto che il suo prodotto con elementi digitali è stato messo a disposizione;

b) a meno che non siano già state fornite le informazioni pertinenti, una notifica delle vulnerabilità, senza indebito ritardo e in ogni caso entro 72 ore dal momento in cui il fabbricante è venuto a conoscenza della vulnerabilità attivamente sfruttata, che fornisca informazioni generali, se disponibili, sul prodotto con elementi digitali interessato, sulla natura generale dello sfruttamento e della vulnerabilità in questione, nonché sulle eventuali misure correttive o di attenuazione adottate e sulle misure correttive o di attenuazione che gli utilizzatori possono adottare, e che indichi anche, se del caso, il grado di sensibilità attribuito dal fabbricante alle informazioni notificate;

c) a meno che non siano già state fornite le informazioni pertinenti, una relazione finale, entro 14 giorni dalla messa a disposizione di una misura correttiva o di attenuazione, che comprenda almeno:

   i) una descrizione della vulnerabilità, compresi la sua gravità e il suo impatto;

   ii) se disponibili, informazioni relative a qualsiasi soggetto malintenzionato che abbia sfruttato o che sfrutti la vulnerabilità;

   iii) informazioni dettagliate relative all'aggiornamento di sicurezza o ad altre misure correttive messe a disposizione per porre rimedio alla vulnerabilità.

3. Un fabbricante notifica simultaneamente al CSIRT designato come coordinatore, conformemente al paragrafo 7 del presente articolo, e all'ENISA, qualsiasi incidente grave che abbia un impatto sulla sicurezza del prodotto con elementi digitali di cui viene a conoscenza. Il fabbricante notifica tale incidente tramite la piattaforma unica di segnalazione istituita a norma dell'articolo 16.

4. Ai fini della notifica di cui al paragrafo 3, il fabbricante presenta:

a) una notifica di preallarme di un incidente grave che ha un impatto sulla sicurezza del prodotto con elementi digitali, senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui il fabbricante ne è venuto a conoscenza, che precisi, come minimo, se si sospetta che l'incidente sia il risultato di atti illegittimi o malevoli, e che indichi, se del caso, gli Stati membri sul cui territorio il fabbricante sia al corrente del fatto che il suo prodotto con elementi digitali è stato messo a disposizione;

b) a meno che non siano già state fornite le informazioni pertinenti, una notifica dell'incidente, senza indebito ritardo e in ogni caso entro 72 ore dal momento in cui il fabbricante ne è venuto a conoscenza, che fornisca informazioni generali, se disponibili, sulla natura dell'incidente, una valutazione iniziale dell'incidente, nonché le eventuali misure correttive o di attenuazione adottate e le misure correttive o di attenuazione che gli utilizzatori possono adottare, e che indichi anche, se del caso, il grado di sensibilità attribuito dal fabbricante alle informazioni notificate;

c) a meno che non siano già state fornite le informazioni pertinenti, una relazione finale entro un mese dalla trasmissione della notifica di incidente di cui alla lettera b), che comprenda almeno:

   i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;

   ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

   iii) le misure di attenuazione adottate e in corso;

5. Ai fini del paragrafo 3, un incidente che ha un impatto sulla sicurezza del prodotto con elementi digitali è considerato grave se:

a) incide negativamente o è in grado di incidere negativamente sulla capacità di un prodotto con elementi digitali di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati o funzioni sensibili o importanti; o

b) ha portato o è in grado di portare all'introduzione o all'esecuzione di un codice maligno in un prodotto con elementi digitali o nei sistemi informativi e di rete di un utilizzatore del prodotto con elementi digitali.

6. Se necessario, il CSIRT designato come coordinatore che ha ricevuto per primo la notifica può chiedere ai fabbricanti di fornire una relazione intermedia sui pertinenti aggiornamenti della situazione sulla vulnerabilità attivamente sfruttata o sull'incidente grave che ha un impatto sulla sicurezza del prodotto con elementi digitali.

7. Le notifiche di cui ai paragrafi 1 e 3 del presente articolo sono trasmesse attraverso la piattaforma unica di segnalazione di cui all'articolo 16 utilizzando uno dei terminali per la notifica elettronica di cui all'articolo 16, paragrafo 1. La notifica è trasmessa utilizzando il terminale per la notifica elettronica del CSIRT designato come coordinatore dello Stato membro in cui i fabbricanti hanno lo stabilimento principale nell'Unione ed è contemporaneamente accessibile all'ENISA.

Ai fini del presente regolamento, si considera che un fabbricante abbia il suo stabilimento principale nell'Unione nello Stato membro in cui sono prevalentemente adottate le decisioni relative alla cibersicurezza dei suoi prodotti con elementi digitali. Se non è possibile determinare detto Stato membro, si considera che lo stabilimento principale sia nello Stato membro in cui il fabbricante ha lo stabilimento con il maggior numero di dipendenti nell'Unione.

Se non ha uno stabilimento principale nell'Unione, il fabbricante trasmette le notifiche di cui ai paragrafi 1 e 3 utilizzando il terminale per la notifica elettronica del CSIRT designato come coordinatore nello Stato membro determinato secondo l'ordine seguente e sulla base delle informazioni a disposizione del fabbricante:

a) lo Stato membro in cui è stabilito il rappresentante autorizzato che agisce per conto del fabbricante per il maggior numero di prodotti con elementi digitali di tale fabbricante;

b) lo Stato membro in cui è stabilito l'importatore che immette sul mercato il maggior numero di prodotti con elementi digitali di tale fabbricante;

c) lo Stato membro in cui è stabilito il distributore che mette a disposizione sul mercato il maggior numero di prodotti con elementi digitali di tale fabbricante;

d) lo Stato membro in cui è situato il maggior numero di utilizzatori di prodotti con elementi digitali di tale fabbricante.

In relazione al terzo comma, lettera d), un fabbricante può presentare notifiche relative a qualsiasi successiva vulnerabilità attivamente sfruttata o incidente grave che ha un impatto sulla sicurezza del prodotto con elementi digitali allo stesso CSIRT designato come coordinatore a cui ha presentato la prima notifica.

8. Dal momento in cui è venuto a conoscenza di una vulnerabilità attivamente sfruttata o di un incidente grave avente un impatto sulla sicurezza del prodotto con elementi digitali, il fabbricante informa gli utilizzatori interessati del prodotto con elementi digitali e, se del caso, tutti gli utilizzatori, di tale vulnerabilità o incidente e, se necessario, di qualsiasi attenuazione dei rischi e misure correttive che gli utilizzatori possono adottare per attenuare l'impatto di tale vulnerabilità o incidente, se del caso in un formato strutturato, leggibile da un dispositivo automatico e che possa essere facilmente elaborato automaticamente. Se il fabbricante non informa tempestivamente gli utilizzatori del prodotto con elementi digitali, i CSIRT designati come coordinatori che hanno ricevuto la notifica possono fornire tali informazioni agli utilizzatori se ritenuto proporzionato e necessario per prevenire o attenuare l'impatto di tale vulnerabilità o incidente.

9. Entro l'11 dicembre 2025 la Commissione adotta atti delegati conformemente all'articolo 61 per integrare il presente regolamento specificando i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione delle notifiche di cui all'articolo 16, paragrafo 2. La Commissione coopera con la rete di CSIRT istituita a norma dell'articolo 15 della direttiva (UE) 2022/2555 e con l'ENISA nella preparazione dei progetti di atti delegati.

10. La Commissione può, mediante atti di esecuzione, specificare ulteriormente il formato e le procedure di trasmissione delle notifiche di cui al presente articolo, nonché agli articoli 15 e 16. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2. La Commissione coopera con la rete di CSIRT e con l'ENISA nella preparazione del progetto di atto delegato.

Articolo 15

Segnalazione volontaria

1. I fabbricanti e altre persone fisiche o giuridiche possono notificare a un CSIRT designato come coordinatore o all'ENISA, su base volontaria, qualsiasi vulnerabilità contenuta in un prodotto con elementi digitali nonché le minacce informatiche che potrebbero incidere sul profilo di rischio di un prodotto con elementi digitali.

2. I fabbricanti e altre persone fisiche o giuridiche possono notificare a un CSIRT designato come coordinatore o all'ENISA, su base volontaria, qualsiasi incidente che abbia un impatto sulla sicurezza del prodotto con elementi digitali e qualsiasi quasi incidente che avrebbe potuto tradursi in un simile incidente.

3. Il CSIRT designato come coordinatore o l'ENISA trattano le notifiche di cui ai paragrafi 1 e 2 del presente articolo secondo la procedura di cui all'articolo 16.

Il CSIRT designato come coordinatore può trattare le notifiche obbligatorie in via prioritaria rispetto alle notifiche volontarie.

4. Qualora una persona fisica o giuridica diversa dal fabbricante notifichi una vulnerabilità attivamente sfruttata o un incidente grave che ha un impatto sulla sicurezza di un prodotto con elementi digitali conformemente al paragrafo 1 o 2, il CSIRT designato come coordinatore ne informa senza indebito ritardo il fabbricante.

5. I CSIRT designati come coordinatori e l'ENISA garantiscono la riservatezza e la protezione adeguata delle informazioni fornite da una persona fisica o giuridica notificante. Fatti salvi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, la segnalazione volontaria non ha l'effetto di imporre alla persona fisica o giuridica notificante alcun obbligo aggiuntivo a cui non sarebbe stata sottoposta se non avesse trasmesso la notifica.

Articolo 16

Istituzione di una piattaforma unica di segnalazione

1. Ai fini delle notifiche di cui all'articolo 14, paragrafi 1 e 3, e all'articolo 15, paragrafi 1 e 2, e per semplificare gli obblighi di segnalazione dei fabbricanti, l'ENISA istituisce una piattaforma unica di segnalazione. Le operazioni quotidiane di tale piattaforma unica di segnalazione sono gestite e mantenute dall'ENISA. L'architettura della piattaforma unica di segnalazione consente agli Stati membri e all'ENISA di predisporre i propri terminali per la notifica elettronica.

2. Dopo aver ricevuto una notifica, il CSIRT designato come coordinatore che ha ricevuto per primo la notifica la diffonde senza ritardo attraverso la piattaforma unica di segnalazione ai CSIRT designati come coordinatori sul cui territorio il fabbricante ha indicato che il prodotto con elementi digitali è stato messo a disposizione.

In circostanze eccezionali e, in particolare, su richiesta del fabbricante e alla luce del grado di sensibilità delle informazioni notificate indicato dal fabbricante a norma dell'articolo 14, paragrafo 2, lettera a), del presente regolamento, la diffusione della notifica può essere ritardata per motivi connessi alla cibersicurezza per un periodo di tempo strettamente necessario, anche nel caso in cui una vulnerabilità sia oggetto di una procedura di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555. Qualora un CSIRT decida di trattenere una notifica, informa immediatamente l'ENISA della decisione e fornisce sia una giustificazione per il trattenimento della notifica sia un'indicazione di quando diffonderà la notifica secondo la procedura di diffusione di cui al presente paragrafo. L'ENISA può sostenere il CSIRT nell'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione della notifica.

In circostanze particolarmente eccezionali, se il fabbricante indica nella notifica di cui all'articolo 14, paragrafo 2, lettera b):

a) che la vulnerabilità notificata è stata attivamente sfruttata da un soggetto malintenzionato e, in base alle informazioni disponibili, non è stata sfruttata in altri Stati membri oltre a quello del CSIRT designato come coordinatore al quale il fabbricante ha notificato la vulnerabilità;

b) che un'ulteriore diffusione immediata della vulnerabilità notificata comporterebbe probabilmente la fornitura di informazioni la cui divulgazione sarebbe contraria agli interessi essenziali di tale Stato membro; o

c) che l'ulteriore diffusione della vulnerabilità notificata si tradurrebbe in un rischio di cibersicurezza elevato e imminente;

unicamente l'informazione dell'avvenuta notifica da parte del fabbricante, le informazioni generali sul prodotto, le informazioni sulla natura generale dello sfruttamento e l'informazione che sono stati sollevati motivi di sicurezza, devono essere rese simultaneamente disponibili a l'ENISA fino a quando la notifica completa non viene diffusa ai CSIRT interessati e all'ENISA. Se l'ENISA, sulla base di tali informazioni, ritiene che vi sia un rischio sistemico capace di incidere sulla sicurezza del mercato interno, raccomanda al CSIRT ricevente di diffondere la notifica completa agli altri CSIRT designati come coordinatori e all'ENISA stessa.

3. Dopo aver ricevuto la notifica di una vulnerabilità attivamente sfruttata in un prodotto con elementi digitali o di un incidente grave che ha un impatto sulla sicurezza di un prodotto con elementi digitali, i CSIRT designati come coordinatori forniscono alle autorità di vigilanza del mercato dei rispettivi Stati membri le informazioni notificate necessarie alle autorità di vigilanza del mercato per adempiere ai loro obblighi a norma del presente regolamento.

4. L'ENISA adotta misure adeguate e proporzionate dal punto di vista tecnico, operativo e organizzativo per gestire i rischi posti alla sicurezza della piattaforma unica di segnalazione e alle informazioni trasmesse o diffuse attraverso la stessa. Essa notifica senza indebito ritardo alla rete di CSIRT e alla Commissione qualsiasi incidente di sicurezza che incida sulla piattaforma unica di segnalazione.

5. L'ENISA, in cooperazione con la rete di CSIRT, fornisce e attua specifiche sulle misure tecniche, operative e organizzative relative all'istituzione, alla manutenzione e al funzionamento sicuro della piattaforma unica di segnalazione di cui al paragrafo 1, comprese almeno le disposizioni in materia di sicurezza relative all'istituzione, al funzionamento e alla manutenzione della piattaforma unica di segnalazione, nonché i terminali per la notifica elettronica istituiti dai CSIRT designati come coordinatori a livello nazionale e dall'ENISA a livello di Unione, compresi gli aspetti procedurali per garantire che, qualora per una vulnerabilità notificata non siano disponibili misure correttive o di attenuazione, le informazioni su tale vulnerabilità siano condivise nel rispetto di rigorosi protocolli di sicurezza e in funzione della necessità di conoscere.

6. Qualora un CSIRT designato come coordinatore sia stato informato di una vulnerabilità attivamente sfruttata nell'ambito di una procedura di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555, il CSIRT designato come coordinatore che ha ricevuto per primo la notifica può ritardare la diffusione della notifica in questione attraverso la piattaforma unica di segnalazione sulla base di motivi giustificati legati alla cibersicurezza per un periodo non superiore a quello strettamente necessario e fino a quando non sia stato dato il consenso alla divulgazione dalle parti coinvolte nella divulgazione coordinata delle vulnerabilità. Tale requisito non impedisce ai fabbricanti di notificare tale vulnerabilità su base volontaria secondo la procedura di cui al presente articolo.

Articolo 17

Altre disposizioni relative alla segnalazione

1. L'ENISA può trasmettere alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), istituita a norma dell'articolo 16 della direttiva (UE) 2022/2555, le informazioni notificate a norma dell'articolo 14, paragrafi 1 e 3, e dell'articolo 15, paragrafi 1 e 2, del presente regolamento se tali informazioni sono pertinenti per la gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala a livello operativo. Al fine di determinare tale pertinenza, l'ENISA può prendere in considerazione le analisi tecniche effettuate dalla rete di CSIRT, se disponibili.

2. Qualora sia necessario sensibilizzare il pubblico per prevenire o attenuare un incidente grave che ha un impatto sulla sicurezza del prodotto con elementi digitali o per gestire un incidente in corso, o qualora la divulgazione dell'incidente sia altrimenti nell'interesse pubblico, il CSIRT designato come coordinatore dello Stato membro pertinente può, previa consultazione del fabbricante interessato e, se del caso, in cooperazione con l'ENISA, informare il pubblico in merito all'incidente o chiedere al fabbricante di farlo.

3. L'ENISA, sulla base delle notifiche ricevute a norma dell'articolo 14, paragrafi 1 e 3, e dell'articolo 15, paragrafi 1 e 2, del presente regolamento elabora, ogni 24 mesi, una relazione tecnica sulle tendenze emergenti in materia di rischi di cibersicurezza nei prodotti con elementi digitali e la presenta al gruppo di cooperazione istituito dall'articolo 14 della direttiva (UE) 2022/2555. La prima relazione di questo tipo è presentata entro 24 mesi dalla data di applicazione degli obblighi stabiliti all'articolo 14, paragrafi 1 e 3. L'ENISA integra le informazioni pertinenti tratte dalle sue relazioni tecniche nella sua relazione sullo stato della cibersicurezza nell'Unione, presentata a norma dell'articolo 18 della direttiva (UE) 2022/2555.

4. La sola notifica in conformità dell'articolo 14, paragrafi 1 e 3, o dell'articolo 15, paragrafi 1 e 2, non sottopone la persona fisica o giuridica notificante a una maggiore responsabilità.

5. Dopo la messa a disposizione di un aggiornamento di sicurezza o l'adozione di un'altra forma di misure correttive o di attenuazione, l'ENISA, d'intesa con il fabbricante del prodotto con elementi digitali interessato, aggiunge la vulnerabilità notificata a norma dell'articolo 14, paragrafo 1, o dell'articolo 15, paragrafo 1, del presente regolamento alla banca dati europea delle vulnerabilità istituita a norma dell'articolo 12 della direttiva (UE) 2022/2555.

6. I CSIRT designati come coordinatori prestano assistenza tecnica in relazione agli obblighi di segnalazione a norma dell'articolo 14 ai fabbricanti e in particolare ai fabbricanti che si qualificano come microimprese o piccole o medie imprese.

Articolo 18

Rappresentanti autorizzati

1. Un fabbricante può nominare, mediante mandato scritto, un rappresentante autorizzato.

2. Gli obblighi di cui all'articolo 13, paragrafi da 1 a 11, paragrafo 12, primo comma, e paragrafo 14, non rientrano nel mandato del rappresentante autorizzato.

3. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fabbricante. Il rappresentante autorizzato fornisce una copia del mandato alle autorità di vigilanza del mercato su richiesta. Tale mandato consente al rappresentante autorizzato di svolgere almeno i seguenti compiti:

a) mantenere a disposizione delle autorità di vigilanza del mercato la dichiarazione di conformità UE di cui all'articolo 28 e la documentazione tecnica di cui all'articolo 31 per un periodo di almeno dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per la durata del periodo di assistenza, se quest'ultimo è superiore;

b) a seguito di una richiesta motivata di un'autorità di vigilanza del mercato, fornire a tale autorità tutte le informazioni e la documentazione necessarie a dimostrare la conformità del prodotto con elementi digitali;

c) collaborare con le autorità di vigilanza del mercato, su richiesta di queste ultime, a qualsiasi azione intrapresa per eliminare i rischi posti da un prodotto con elementi digitali che rientra nel suo mandato.

Articolo 19

Obblighi degli importatori

1. Gli importatori immettono sul mercato solo prodotti con elementi digitali conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e laddove i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte II.

2. Prima di immettere un prodotto con elementi digitali sul mercato gli importatori si accertano che:

a) il fabbricante abbia eseguito le procedure di valutazione della conformità appropriate di cui all'articolo 32;

b) il fabbricante abbia redatto la documentazione tecnica;

c) il prodotto con elementi digitali rechi la marcatura CE di cui all'articolo 30 e sia accompagnato dalla dichiarazione di conformità UE di cui all'articolo 13, paragrafo 20, e dalle informazioni e dalle istruzioni per l'utilizzatore di cui all'allegato II, redatte in una lingua facilmente comprensibile per gli utilizzatori e le autorità di vigilanza del mercato;

d) il fabbricante abbia soddisfatto i requisiti di cui all'articolo 13, paragrafi 15, 16 e 19.

Ai fini del presente paragrafo, gli importatori sono in grado di fornire la documentazione necessaria a comprovare il rispetto dei requisiti di cui al presente articolo.

3. Qualora ritenga o abbia motivo di credere che un prodotto con elementi digitali o i processi messi in atto dal fabbricante non siano conformi al presente regolamento, l'importatore non immette il prodotto sul mercato fino a quando il prodotto o i processi messi in atto dal fabbricante non siano stati resi conformi al presente regolamento. Inoltre, se il prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, l'importatore ne informa il fabbricante e le autorità di vigilanza del mercato.

Qualora abbia motivo di credere che un prodotto con elementi digitali possa presentare un rischio di cibersicurezza significativo alla luce di fattori di rischio non tecnici, l'importatore ne informa le autorità di vigilanza del mercato. Non appena ricevute tali informazioni, le autorità di vigilanza del mercato seguono le procedure di cui all'articolo 54, paragrafo 2.

4. Gli importatori indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato, l'indirizzo postale, l'indirizzo di posta elettronica o altro contatto digitale nonché, se disponibile, il sito web ai quali possono essere contattati sul prodotto con elementi digitali oppure sull'imballaggio o in un documento di accompagnamento del prodotto con elementi digitali. I dati di recapito sono redatti in una lingua facilmente comprensibile dagli utilizzatori e dalle autorità di vigilanza del mercato.

5. Gli importatori che hanno la certezza o hanno motivo di credere che un prodotto con elementi digitali che hanno immesso sul mercato non sia conforme al presente regolamento adottano immediatamente le misure correttive necessarie per far sì che tale prodotto con elementi digitali sia reso conforme al presente regolamento, oppure, se del caso, per ritirare o richiamare il prodotto.

Quando vengono a conoscenza di una vulnerabilità nel prodotto con elementi digitali, gli importatori ne informano il fabbricante senza indebito ritardo. Inoltre, se il prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, gli importatori ne informano immediatamente le autorità di vigilanza del mercato degli Stati membri in cui hanno messo a disposizione sul mercato il prodotto con elementi digitali, dando in particolare informazioni dettagliate sulla non conformità e su eventuali misure correttive adottate.

6. Gli importatori mantengono una copia della dichiarazione di conformità UE a disposizione delle autorità di vigilanza del mercato per un periodo di almeno dieci anni dalla data di immissione sul mercato del prodotto con elementi digitali o per la durata del periodo di assistenza, se quest'ultimo è superiore, e si accertano che la documentazione tecnica possa essere messa a disposizione di tali autorità, su richiesta.

7. A seguito di una richiesta motivata di un'autorità di vigilanza del mercato, gli importatori forniscono a quest'ultima, in formato cartaceo o elettronico, tutte le informazioni e la documentazione necessarie a dimostrare la conformità del prodotto con elementi digitali ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, nonché la conformità dei processi messi in atto dal fabbricante ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte II, in una lingua che

possa essere facilmente compresa da tale autorità. Essi cooperano con tale autorità, su sua richiesta, a qualsiasi misura adottata per eliminare i rischi di cibersicurezza presentati da un prodotto con elementi digitali da essi immesso sul mercato.

8. Qualora venga a conoscenza del fatto che il fabbricante di un prodotto con elementi digitali ha cessato l'attività e di conseguenza non è in grado di rispettare gli obblighi previsti dal presente regolamento, l'importatore di tale prodotto ne informa le autorità di vigilanza del mercato competenti nonché, con qualsiasi mezzo disponibile e nella misura del possibile, gli utilizzatori dei prodotti con elementi digitali immessi sul mercato.

Articolo 20

Obblighi dei distributori

1. Quando mettono un prodotto con elementi digitali a disposizione sul mercato, i distributori esercitano la dovuta diligenza per rispettare i requisiti stabiliti dal presente regolamento.

2. Prima di mettere un prodotto con elementi digitali a disposizione sul mercato, i distributori verificano che:

a) il prodotto con elementi digitali rechi la marcatura CE;

b) il fabbricante e l'importatore abbiano rispettato gli obblighi previsti dall'articolo 13, paragrafi 15, 16, 18, 19 e 20, e dall'articolo 19, paragrafo 4, e abbiano trasmesso tutta la documentazione necessaria al distributore.

3. Se un distributore ritiene o ha motivo di credere, sulla base delle informazioni in suo possesso, che un prodotto con elementi digitali o i processi messi in atto dal fabbricante non siano conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I, il distributore non mette il prodotto con elementi digitali a disposizione sul mercato fino a quando il prodotto o i processi messi in atto dal fabbricante non siano stati resi conformi al presente regolamento. Inoltre, quando il prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, il distributore ne informa, senza indebito ritardo, il fabbricante e le autorità di vigilanza del mercato.

4. I distributori che hanno la certezza o hanno motivo di credere, sulla base delle informazioni in loro possesso, che un prodotto con elementi digitali che hanno messo a disposizione sul mercato o i processi messi in atto dal suo fabbricante non siano conformi al presente regolamento si assicurano che siano adottate le misure correttive necessarie per rendere conformi tale prodotto con elementi digitali o i processi messi in atto dal suo fabbricante oppure, se del caso, per ritirare o richiamare il prodotto.

Quando vengono a conoscenza di una vulnerabilità nel prodotto con elementi digitali, i distributori ne informano il fabbricante senza indebito ritardo. Inoltre, se il prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, i distributori ne informano immediatamente le autorità di vigilanza del mercato degli Stati membri in cui hanno messo a disposizione sul mercato il prodotto con elementi digitali, dando in particolare informazioni dettagliate sulla non conformità e su eventuali misure correttive adottate.

5. A seguito di una richiesta motivata di un'autorità di vigilanza del mercato, i distributori forniscono, in formato cartaceo o elettronico, tutte le informazioni e la documentazione necessarie a dimostrare la conformità del prodotto con elementi digitali e dei processi messi in atto dal suo fabbricante al presente regolamento in una lingua che possa essere facilmente compresa da tale autorità. Essi cooperano con tale autorità, su sua richiesta, a qualsiasi misura adottata per eliminare i rischi di cibersicurezza presentati da un prodotto con elementi digitali da essi messo a disposizione sul mercato.

6. Qualora venga a conoscenza, sulla base delle informazioni in suo possesso, del fatto che il fabbricante di un prodotto con elementi digitali ha cessato l'attività e di conseguenza non è in grado di rispettare gli obblighi previsti dal presente regolamento, il distributore di tale prodotto ne informa, senza indebito ritardo, le autorità di vigilanza del mercato competenti nonché, con qualsiasi mezzo disponibile e nella misura del possibile, gli utilizzatori dei prodotti con elementi digitali immessi sul mercato.

Articolo 21

Casi in cui gli obblighi dei fabbricanti si applicano agli importatori e ai distributori

Un importatore o distributore è ritenuto un fabbricante ai fini del presente regolamento, ed è soggetto agli obblighi di cui agli articoli 13 e 14, quando immette sul mercato un prodotto con elementi digitali con il proprio nome o marchio commerciale o apporta una modifica sostanziale a un prodotto con elementi digitali già immesso sul mercato.

Articolo 22

Altri casi in cui si applicano gli obblighi dei fabbricanti

1. Una persona fisica o giuridica, diversa dal fabbricante, dall'importatore o dal distributore, che apporta una modifica sostanziale a un prodotto con elementi digitali e mette tale prodotto a disposizione sul mercato è considerata un fabbricante ai fini del presente regolamento.

2. La persona di cui al paragrafo 1 del presente articolo è soggetta agli obblighi di cui agli articoli 13 e 14 per la parte del prodotto con elementi digitali interessata da tale modifica sostanziale oppure, se la modifica sostanziale incide sulla cibersicurezza del prodotto con elementi digitali nel suo complesso, per l'intero prodotto.

Articolo 23

Identificazione degli operatori economici

1. Gli operatori economici, su richiesta, forniscono alle autorità di vigilanza del mercato le informazioni seguenti:

a) il nome e l'indirizzo di qualsiasi operatore economico che abbia fornito loro un prodotto con elementi digitali;

b) se disponibili, il nome e l'indirizzo di qualsiasi operatore economico cui essi abbiano fornito un prodotto con elementi digitali.

2. Gli operatori economici si assicurano di essere in grado di presentare le informazioni di cui al paragrafo 1 per dieci anni dal momento in cui sia stato loro fornito un prodotto con elementi digitali e per dieci anni dal momento in cui essi abbiano fornito il prodotto con elementi digitali.

Articolo 24

Obblighi dei gestori di software open source

1. I gestori di software open source mettono in atto e documentano in modo verificabile una politica in materia di cibersicurezza per promuovere lo sviluppo di un prodotto con elementi digitali sicuro nonché una gestione efficace delle vulnerabilità da parte degli sviluppatori di tale prodotto. Tale politica promuove inoltre la segnalazione volontaria di vulnerabilità di cui all'articolo 15 da parte degli sviluppatori di tale prodotto e tiene conto della natura specifica del software open source e delle disposizioni giuridiche e organizzative cui è soggetto. La politica include, in particolare, aspetti relativi alla documentazione, al trattamento e alla correzione delle vulnerabilità e promuove la condivisione di informazioni relative alle vulnerabilità individuate nell'ambito della comunità open source.

2. I gestori di software open source cooperano con le autorità di vigilanza del mercato, su loro richiesta, al fine di attenuare i rischi di cibersicurezza presentati da un prodotto con elementi digitali che si qualificano come software liberi e open source.

A seguito di una richiesta motivata di un'autorità di vigilanza del mercato, i gestori di software open source forniscono a tale autorità, in una lingua che possa essere facilmente compresa da quest'ultima, la documentazione di cui al paragrafo 1, in formato cartaceo o elettronico.

3. Gli obblighi di cui all'articolo 14, paragrafo 1, si applicano ai gestori di software open source nella misura in cui sono coinvolti nello sviluppo dei prodotti con elementi digitali. Gli obblighi di cui all'articolo 14, paragrafi 3 e 8, si applicano ai gestori di software open source nella misura in cui incidenti gravi che hanno un impatto sulla sicurezza dei prodotti con elementi digitali incidano sui sistemi informativi e di rete forniti da tali gestori di software open source per lo sviluppo di tali prodotti.

Articolo 25

Attestazione di sicurezza dei software liberi e open source

Al fine di agevolare l'obbligo di dovuta diligenza di cui all'articolo 13, paragrafo 5, in particolare per quanto riguarda i fabbricanti che integrano componenti software liberi e open source nei loro prodotti con elementi digitali, alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 61 al fine di integrare il presente regolamento istituendo programmi volontari di attestazione di sicurezza che consentano agli sviluppatori o agli utilizzatori di prodotti con elementi digitali che si qualificano come software liberi e open source, nonché ad altri soggetti terzi, di valutare la conformità di tali prodotti a tutti o a determinati requisiti essenziali di cibersicurezza o ad altri obblighi di cui al presente regolamento.

Articolo 26

Orientamenti

1. Al fine di agevolare l'attuazione e di assicurarne la coerenza, la Commissione pubblica orientamenti per assistere gli operatori economici nell'applicazione del presente regolamento, con particolare attenzione all'agevolazione della conformità da parte delle microimprese e delle piccole e medie imprese.

2. Qualora intenda fornire gli orientamenti di cui al paragrafo 1, la Commissione affronta almeno gli aspetti seguenti:

a) l'ambito di applicazione del presente regolamento, con particolare attenzione alle soluzioni di elaborazione dati da remoto e ai software liberi e open-source;

b) l'applicazione di periodi di assistenza in relazione a particolari categorie di prodotti con elementi digitali;

c) orientamenti destinati ai fabbricanti soggetti al presente regolamento che sono anche soggetti ad altre normative di armonizzazione dell'Unione diverse dal presente regolamento o ad altri atti giuridici dell'Unione correlati;

d) il concetto di modifica sostanziale.

La Commissione mantiene inoltre un elenco facilmente fruibile degli atti delegati e di esecuzione adottati a norma del presente regolamento.

3. Nell'elaborare gli orientamenti a norma del presente articolo, la Commissione consulta i portatori di interessi pertinenti.

CAPO III

CONFORMITÀ DEL PRODOTTO CON ELEMENTI DIGITALI

Articolo 27

Presunzione di conformità

1. I prodotti con elementi digitali e i processi messi in atto dal fabbricante che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* si presumono conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I oggetto di tali norme o parti di esse.

In conformità dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, la Commissione chiede a una o più organizzazioni europee di normazione di elaborare norme armonizzate per i requisiti essenziali di cibersicurezza di cui all'allegato I del presente regolamento. Nel preparare richieste di normazione per il presente regolamento, la Commissione si adopera per tenere conto delle norme europee ed internazionali esistenti in materia di cibersicurezza, siano esse in vigore o in corso di elaborazione, al fine di semplificare lo sviluppo delle norme armonizzate, ai sensi del regolamento (UE) n. 1025/2012.

2. Alla Commissione è conferito il potere di adottare atti di esecuzione che stabiliscono specifiche comuni relative ai requisiti tecnici che forniscono i mezzi per soddisfare i requisiti essenziali di cibersicurezza di cui all'allegato I per i prodotti con elementi digitali rientranti nell'ambito di applicazione del presente regolamento.

Tali atti di esecuzione sono adottati solo laddove siano soddisfatte le condizioni seguenti:

a) la Commissione ha richiesto, a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, a una o più organizzazioni europee di normazione di redigere una norma armonizzata per i requisiti essenziali di cibersicurezza di cui all'allegato I, e:

   i) la richiesta non è stata accettata;

   ii) le norme armonizzate relative a tale richiesta non sono fornite entro il termine stabilito conformemente all'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012; o

   iii) le norme armonizzate non sono conformi alla richiesta; e

b) nessun riferimento a norme armonizzate che contemplano i requisiti essenziali di cibersicurezza pertinenti di cui all'allegato I del presente regolamento è stato pubblicato nella *Gazzetta ufficiale dell'Unione europea* conformemente al regolamento (UE) n. 1025/2012 e non si prevede la pubblicazione di tale riferimento entro un termine ragionevole.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

3. Prima di preparare il progetto di atto di esecuzione di cui al paragrafo 2 del presente articolo, la Commissione informa il comitato di cui all'articolo 22 del regolamento (UE) n. 1025/2012 di ritenere soddisfatte le condizioni di cui al paragrafo 2 del presente articolo.

4. Nel preparare il progetto di atto di esecuzione di cui al paragrafo 2, la Commissione tiene conto dei pareri degli organi competenti e consulta debitamente tutti i portatori di interessi pertinenti.

5. I prodotti con elementi digitali e i processi messi in atto dal fabbricante che sono conformi alle specifiche comuni stabilite dagli atti di esecuzione di cui al paragrafo 2 del presente articolo, o a parti di esse, si presumono conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I oggetto di tali specifiche comuni o di loro parti.

6. Qualora una norma armonizzata sia adottata da un'organizzazione europea di normazione e proposta alla Commissione al fine di pubblicarne il riferimento nella *Gazzetta ufficiale dell'Unione europea*, la Commissione valuta la norma armonizzata conformemente al regolamento (UE) n. 1025/2012. Quando un riferimento a una norma armonizzata è pubblicato nella *Gazzetta ufficiale dell'Unione europea*, la Commissione abroga gli atti di esecuzione di cui al paragrafo 2 del presente articolo, o parti di essi, che riguardano gli stessi requisiti essenziali di cibersicurezza contemplati da tale norma armonizzata.

7. Qualora uno Stato membro ritenga che una specifica comune non soddisfi completamente i requisiti essenziali di cibersicurezza di cui all'allegato I, esso ne informa la Commissione presentando una spiegazione dettagliata. La Commissione valuta tale spiegazione dettagliata e, se del caso, modifica l'atto di esecuzione che stabilisce la specifica comune in questione.

8. I prodotti con elementi digitali e i processi messi in atto dal fabbricante per i quali sono stati rilasciati un certificato o una dichiarazione di conformità UE nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma del regolamento (UE) 2019/881 si presumono conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I, nella misura in cui tali requisiti siano contemplati dal certificato europeo di cibersicurezza o dalla dichiarazione di conformità UE o da loro parti.

9. Alla Commissione è conferito il potere di adottare atti delegati ai sensi dell'articolo 61 del presente regolamento per integrare il presente regolamento specificando i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che possono essere utilizzati per dimostrare la conformità dei prodotti con elementi digitali ai requisiti essenziali di cibersicurezza o a parti di essi di cui all'allegato I del presente regolamento. Inoltre l'emissione di un certificato europeo di cibersicurezza rilasciato nell'ambito di tali sistemi con un livello di affidabilità almeno «sostanziale» sopprime l'obbligo per un fabbricante di effettuare una valutazione della conformità da parte di terzi per i requisiti corrispondenti, come previsto dall'articolo 32, paragrafo 2, lettere a) e b), e dall'articolo 32, paragrafo 3), lettere a) e b), del presente regolamento.

Articolo 28

Dichiarazione di conformità UE

1. La dichiarazione di conformità UE è redatta dai fabbricanti in conformità dell'articolo 13, paragrafo 12, e attesta il rispetto dei requisiti essenziali di cibersicurezza applicabili di cui all'allegato I.

2. La dichiarazione di conformità UE ha la struttura tipo di cui all'allegato V e contiene gli elementi specificati nelle pertinenti procedure di valutazione della conformità di cui all'allegato VIII. Tale dichiarazione è opportunamente aggiornata. È resa disponibile nelle lingue richieste dallo Stato membro sul cui mercato il prodotto con elementi digitali è immesso o messo a disposizione sul mercato.

La dichiarazione di conformità UE semplificata di cui all'articolo 13, paragrafo 20, ha la struttura tipo di cui all'allegato VI. È resa disponibile nelle lingue richieste dallo Stato membro sul cui mercato il prodotto con elementi digitali è immesso o messo a disposizione sul mercato.

3. Se al prodotto con elementi digitali si applicano più atti giuridici dell'Unione che prescrivono una dichiarazione di conformità UE, è redatta un'unica dichiarazione di conformità UE in relazione a tutti questi atti giuridici dell'Unione. La dichiarazione contiene gli estremi degli atti giuridici dell'Unione in questione, compresi i riferimenti della loro pubblicazione.

4. Con la dichiarazione di conformità UE il fabbricante si assume la responsabilità della conformità del prodotto con elementi digitali.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 61 per integrare il presente regolamento aggiungendo elementi al contenuto minimo della dichiarazione di conformità UE di cui all'allegato V per tenere conto degli sviluppi tecnologici.

Articolo 29

Principi generali della marcatura CE

La marcatura CE è soggetta ai principi generali stabiliti all'articolo 30 del regolamento (CE) n. 765/2008.

Articolo 30

Regole e condizioni per l'apposizione della marcatura CE

1. La marcatura CE è apposta sul prodotto con elementi digitali in modo visibile, leggibile e indelebile. Qualora ciò non sia possibile o la natura del prodotto con elementi digitali non lo consenta, essa è apposta sull'imballaggio e sulla dichiarazione di conformità UE di cui all'articolo 28 che accompagna il prodotto con elementi digitali. Per i prodotti con elementi digitali sotto forma di software, la marcatura CE è apposta sulla dichiarazione di conformità UE di cui all'articolo 28 o sul sito web che accompagna il prodotto software. In quest'ultimo caso, la sezione pertinente del sito web è facilmente e direttamente accessibile ai consumatori.

2. A seconda della natura del prodotto con elementi digitali, l'altezza della marcatura CE apposta su di esso può essere inferiore a 5 mm, purché rimanga visibile e leggibile.

3. La marcatura CE è apposta sul prodotto con elementi digitali prima della sua immissione sul mercato. Può essere seguita da un pittogramma o da qualsiasi altro marchio che indichi un rischio di cibersicurezza o un impiego particolar stabilito negli atti di esecuzione di cui al paragrafo 6.

4. La marcatura CE è seguita dal numero di identificazione dell'organismo notificato, qualora quest'ultimo partecipi alla procedura di valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'articolo 32.

Il numero di identificazione dell'organismo notificato è apposto dall'organismo stesso o, in base alle istruzioni di quest'ultimo, dal fabbricante o dal rappresentante autorizzato del fabbricante.

5. Gli Stati membri si avvalgono dei meccanismi esistenti per garantire un'applicazione corretta del regime che disciplina la marcatura CE e promuovono le azioni opportune contro l'uso improprio di tale marcatura. Qualora il prodotto con elementi digitali sia soggetto ad altre normative di armonizzazione dell'Unione diverse dal presente regolamento che prevedono l'apposizione della marcatura CE, questa indica che il prodotto rispetta anche i requisiti stabiliti in tali altre normative di armonizzazione dell'Unione.

6. La Commissione può, mediante atti di esecuzione, stabilire specifiche tecniche per le etichette, i pittogrammi o qualsiasi altro marchio relativo alla sicurezza dei prodotti con elementi digitali, i loro periodi di assistenza e meccanismi per promuoverne l'uso, nonché per sensibilizzare il pubblico in merito alla sicurezza dei prodotti con elementi digitali. Nell'elaborare i progetti di atti di esecuzione, la Commissione consulta i portatori di interessi pertinenti e, laddove sia stato già stabilito a norma dell'articolo 52, paragrafo 15, l'ADCO. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

Articolo 31

Documentazione tecnica

1. La documentazione tecnica contiene tutti i dati o i dettagli pertinenti relativi ai mezzi utilizzati dal fabbricante per garantire che il prodotto con elementi digitali e i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I. Essa contiene almeno gli elementi di cui all'allegato VII.

2. La documentazione tecnica è redatta prima dell'immissione sul mercato del prodotto con elementi digitali ed è costantemente aggiornata, se del caso, almeno per tutta la durata del periodo di assistenza.

3. Per i prodotti con elementi digitali di cui all'articolo 12 che sono soggetti anche ad altri atti giuridici dell'Unione che prevedono documentazione tecnica, è redatta un'unica documentazione tecnica contenente le informazioni di cui all'allegato VII e le informazioni richieste dai rispettivi atti giuridici dell'Unione.

4. La documentazione tecnica e la corrispondenza relativa a qualsiasi procedura di valutazione della conformità sono redatte in una delle lingue ufficiali dello Stato membro in cui è stabilito l'organismo notificato o in una lingua accettata da quest'ultimo.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 61 per integrare il presente regolamento aggiungendo elementi da includere nella documentazione tecnica di cui all'allegato VII, al fine di tenere conto degli sviluppi tecnologici e degli sviluppi riscontrati nel processo di attuazione del presente regolamento. A tal fine la Commissione si adopera affinché gli oneri amministrativi a carico delle microimprese e delle piccole e medie imprese siano proporzionati.

Articolo 32

Procedure di valutazione della conformità per prodotti con elementi digitali

1. Il fabbricante effettua una valutazione della conformità del prodotto con elementi digitali e dei processi messi in atto dal fabbricante per determinare se sono soddisfatti i requisiti essenziali di cibersicurezza di cui all'allegato I. Il fabbricante dimostra la conformità ai requisiti essenziali di cibersicurezza utilizzando una delle procedure seguenti:

a) la procedura di controllo interno (basata sul modulo A) di cui all'allegato VIII;

b) la procedura di esame UE del tipo (basata sul modulo B) di cui all'allegato VIII, seguita dalla conformità al tipo UE basata sul controllo interno della produzione (basata sul modulo C) di cui all'allegato VIII;

c) una valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'allegato VIII; o

d) ove disponibile e applicabile, un sistema europeo di certificazione della cibersicurezza a norma dell'articolo 27, paragrafo 9.

2. Se per la valutazione della conformità del prodotto con elementi digitali importante rientrante nella classe I di cui all'allegato III e dei processi messi in atto dal suo fabbricante ai requisiti essenziali di cibersicurezza di cui all'allegato I il fabbricante non ha applicato o ha applicato solo in parte norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza con un livello di affidabilità almeno «sostanziale» di cui all'articolo 27, o nel caso in cui non esistano tali norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza, il prodotto con elementi digitali in questione e i processi messi in atto dal fabbricante sono sottoposti, per verificarne la conformità a tali requisiti essenziali di cibersicurezza, a una delle procedure seguenti:

a) la procedura di esame UE del tipo (basata sul modulo B) di cui all'allegato VIII, seguita dalla conformità al tipo UE basata sul controllo interno della produzione (basata sul modulo C) di cui all'allegato VIII; o

b) la valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'allegato VIII.

3. Se il prodotto è un prodotto con elementi digitali importante rientrante nella classe II, come indicato nell'allegato III, il fabbricante dimostra la conformità ai requisiti essenziali di cibersicurezza di cui all'allegato I utilizzando una delle procedure seguenti:

a) la procedura di esame UE del tipo (basata sul modulo B) di cui all'allegato VIII, seguita dalla conformità al tipo UE basata sul controllo interno della produzione (basata sul modulo C) di cui all'allegato VIII;

b) la valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'allegato VIII; o

c) ove disponibile e applicabile, un sistema europeo di certificazione della cibersicurezza a norma dell'articolo 27, paragrafo 9, del presente regolamento con un livello di affidabilità almeno «sostanziale» ai sensi del regolamento (UE) 2019/881.

4. I prodotti con elementi digitali critici di classe II elencati nell'allegato IV dimostrano la conformità ai requisiti essenziali di cibersicurezza di cui all'allegato I utilizzando una delle procedure seguenti:

a) un sistema europeo di certificazione della cibersicurezza a norma dell'articolo 8, paragrafo 1; o

b) se le condizioni di cui all'articolo 8, paragrafo 1, non sono soddisfatte, una delle procedure di cui al paragrafo 3 del presente articolo.

5. I fabbricanti di prodotti con elementi digitali che si qualificano come software liberi e open-source che rientrano nelle categorie di cui all'allegato III sono in grado di dimostrare la conformità ai requisiti essenziali i cibersicurezza di cui all'allegato I utilizzando una delle procedure di cui al paragrafo 1 del presente articolo, a condizione che la documentazione tecnica di cui all'articolo 31 sia messa a disposizione del pubblico al momento dell'immissione sul mercato di tali prodotti.

6. Si dovrebbe tener conto degli interessi e delle esigenze specifici delle microimprese e delle piccole e medie imprese, comprese le start-up, nel definire le tariffe per le procedure di valutazione della conformità e tali tariffe sono ridotte proporzionalmente agli interessi e alle esigenze specifici di tali imprese.

Articolo 33

Misure di sostegno per le microimprese e le piccole e medie imprese, comprese le start-up

1. Gli Stati membri intraprendono, se del caso, le azioni seguenti, adattate alle esigenze delle microimprese e delle piccole imprese:

a) organizzano attività specifiche di sensibilizzazione e formazione circa l'applicazione del presente regolamento;

b) istituiscono un canale dedicato per la comunicazione con le microimprese e le piccole imprese e, se del caso, con le autorità pubbliche locali per fornire consulenza e rispondere alle domande sull'attuazione del presente regolamento;

c) sostengono le attività di prova e di valutazione della conformità, se del caso anche con il sostegno del Centro europeo di competenza per la cibersicurezza.

2. Gli Stati membri possono, se del caso, istituire spazi di sperimentazione normativa per la ciberresilienza. Tali spazi di sperimentazione normativa prevedono ambienti di prova controllati per prodotti innovativi con elementi digitali al fine di facilitarne lo sviluppo, la progettazione, la convalida e le prove ai fini della conformità al presente regolamento per un periodo di tempo limitato precedente all'immissione sul mercato. La Commissione e, se del caso, l'ENISA possono fornire sostegno tecnico, consulenza e strumenti per l'istituzione e il funzionamento degli spazi di sperimentazione normativa. Essi sono istituiti sotto la supervisione, l'orientamento e il sostegno diretti delle autorità di vigilanza del mercato. Gli Stati membri informano la Commissione e le altre autorità di vigilanza del mercato dell'istituzione di uno spazio di sperimentazione normativa attraverso l'ADCO. Gli spazi di sperimentazione normativa non pregiudicano i poteri correttivi e di sorveglianza delle autorità competenti. Gli Stati membri garantiscono un accesso aperto, equo e trasparente agli spazi di sperimentazione normativa e, in particolare, ne facilitano l'accesso delle microimprese e delle piccole imprese, comprese le start-up.

3. Conformemente all'articolo 26, la Commissione fornisce orientamenti alle microimprese e alle piccole e medie imprese in relazione all'attuazione del presente regolamento.

4. La Commissione promuove il sostegno finanziario disponibile nel quadro normativo dei programmi dell'Unione esistenti, in particolare al fine di alleggerire l'onere finanziario per le microimprese e le piccole imprese.

5. Le microimprese e le piccole imprese possono fornire tutti gli elementi della documentazione tecnica specificata nell'allegato VII avvalendosi di un formato semplificato. A tal fine la Commissione specifica, mediante atti di esecuzione, il modulo di documentazione tecnica semplificata destinato alle esigenze delle microimprese e delle piccole imprese, comprese le modalità in cui devono essere forniti gli elementi di cui all'allegato VII. Se una microimpresa o una piccola impresa sceglie di fornire le informazioni di cui all'allegato VII in modo semplificato, utilizza il modulo di cui al presente paragrafo. Gli organismi notificati accettano tale modulo ai fini della valutazione della conformità.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

Articolo 34

Accordi sul reciproco riconoscimento

Tenuto conto del livello di sviluppo tecnico e dell'approccio in materia di valutazione della conformità di un paese terzo, l'Unione può concludere accordi sul reciproco riconoscimento con paesi terzi, conformemente all'articolo 218 TFUE, al fine di promuovere e agevolare il commercio internazionale.

CAPO IV

NOTIFICA DEGLI ORGANISMI DI VALUTAZIONE DELLA CONFORMITÀ

Articolo 35

Notifica

1. Gli Stati membri notificano alla Commissione e agli altri Stati membri gli organismi autorizzati a effettuare valutazioni della conformità a norma del presente regolamento.

2. Gli Stati membri si adoperano per garantire, entro l'11 dicembre 2026, che nell'Unione vi sia un numero sufficiente di organismi notificati per effettuare valutazioni della conformità, al fine di evitare strozzature e ostacoli all'ingresso nel mercato.

Articolo 36

Autorità di notifica

1. Ogni Stato membro designa un'autorità di notifica responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e il loro controllo, anche per quanto riguarda l'ottemperanza all'articolo 41.

2. Gli Stati membri possono decidere che la valutazione e il controllo di cui al paragrafo 1 siano eseguiti da un organismo nazionale di accreditamento ai sensi e in conformità del regolamento (CE) n. 765/2008.

3. Se l'autorità di notifica delega o altrimenti affida la valutazione, notifica o il controllo di cui al paragrafo 1 a un organismo che non è un ente pubblico, detto organismo è una persona giuridica e rispetta *mutatis mutandis* le disposizioni di cui all'articolo 37. Inoltre, tale organismo predispone disposizioni per coprire le responsabilità risultanti dalle sue attività.

4. L'autorità di notifica si assume la piena responsabilità per i compiti svolti dall'organismo di cui al paragrafo 3.

Articolo 37

Requisiti relativi alle autorità di notifica

1. L'autorità di notifica è istituita in modo che non sorgano conflitti di interesse con gli organismi di valutazione della conformità.

2. L'autorità di notifica è organizzata e funziona in modo che siano salvaguardate l'obiettività e l'imparzialità delle sue attività.

3. L'autorità di notifica è organizzata in modo che ogni decisione relativa alla notifica di un organismo di valutazione della conformità sia adottata da persone competenti, diverse da quelle che hanno effettuato la valutazione.

4. L'autorità di notifica non offre e non fornisce attività svolte dagli organismi di valutazione della conformità o servizi di consulenza su base commerciale o concorrenziale.

5. L'autorità di notifica salvaguarda la riservatezza delle informazioni ottenute.

6. L'autorità di notifica ha a sua disposizione un numero di dipendenti competenti sufficiente per l'adeguata esecuzione dei suoi compiti.

Articolo 38

Obbligo di informazione a carico delle autorità di notifica

1. Gli Stati membri informano la Commissione delle loro procedure per la valutazione e la notifica degli organismi di valutazione della conformità e per il controllo degli organismi notificati, nonché di qualsiasi modifica delle stesse.

2. La Commissione rende pubbliche le informazioni di cui al paragrafo 1.

Articolo 39

Requisiti relativi agli organismi notificati

1. Ai fini della notifica, l'organismo di valutazione della conformità rispetta i requisiti di cui ai paragrafi da 2 a 12.

2. L'organismo di valutazione della conformità è istituito a norma della legge nazionale e ha personalità giuridica.

3. L'organismo di valutazione della conformità è un organismo terzo indipendente dall'organizzazione o dal prodotto con elementi digitali che valuta.

Un organismo appartenente a un'associazione d'imprese o a una federazione professionale che rappresenta imprese coinvolte nella progettazione, nello sviluppo, nella produzione, nella fornitura, nell'assemblaggio, nell'utilizzo o nella manutenzione di prodotti con elementi digitali che esso valuta può essere considerato un organismo terzo, a condizione che ne siano dimostrate l'indipendenza e l'assenza di qualsiasi conflitto di interesse.

4. L'organismo di valutazione della conformità, i suoi alti dirigenti e il personale incaricato di svolgere i compiti di valutazione della conformità non sono né il progettista, né lo sviluppatore, né il fabbricante, né il fornitore, né l'importatore, né il distributore, né l'installatore, né l'acquirente, né il proprietario, né l'utilizzatore o il responsabile della manutenzione dei prodotti con elementi digitali che essi valutano, né il rappresentante autorizzato di uno di questi soggetti. Ciò non preclude l'uso di prodotti valutati che sono necessari per il funzionamento dell'organismo di valutazione della conformità né l'uso di tali prodotti a scopi personali.

L'organismo di valutazione della conformità, i suoi alti dirigenti e il personale incaricato di svolgere i compiti di valutazione della conformità non intervengono direttamente nella progettazione, nello sviluppo, nella produzione, nell'importazione, nella distribuzione, nella commercializzazione, nell'installazione, nell'utilizzo o nella manutenzione dei prodotti con elementi digitali che essi valutano, né rappresentano i soggetti impegnati in tali attività. Essi non devono intraprendere alcuna attività che possa essere in conflitto con la loro indipendenza di giudizio o integrità riguardo alle attività di valutazione della conformità per cui sono notificati. Ciò vale in particolare per i servizi di consulenza.

Gli organismi di valutazione della conformità si accertano che le attività delle loro affiliate o dei loro subappaltatori non si ripercuotano sulla riservatezza, sull'obiettività o sull'imparzialità delle loro attività di valutazione della conformità.

5. Gli organismi di valutazione della conformità e il loro personale eseguono le operazioni di valutazione della conformità con il massimo dell'integrità professionale e con la competenza tecnica richiesta nel campo specifico e sono liberi da qualsivoglia pressione e incentivo, soprattutto di ordine finanziario, che possa influenzare il loro giudizio o i risultati delle loro attività di valutazione della conformità, in particolare da persone o gruppi di persone interessati ai risultati di tali attività.

6. L'organismo di valutazione della conformità è in grado di svolgere tutti i compiti di valutazione della conformità di cui all'allegato VIII e per i quali è stato notificato, indipendentemente dal fatto che tali compiti siano eseguiti dall'organismo stesso o per suo conto e sotto la sua responsabilità.

In ogni momento, per ogni procedura di valutazione della conformità e per ogni tipo o categoria di prodotti con elementi digitali per i quali è stato notificato, l'organismo di valutazione della conformità ha a sua disposizione:

a) il necessario personale avente conoscenze tecniche ed esperienza sufficiente e appropriata per eseguire i compiti di valutazione della conformità;

b) la necessaria descrizione delle procedure in base alle quali deve essere svolta la valutazione della conformità, al fine di garantire la trasparenza e la capacità di riprodurre tali procedure. Esso dispone di politiche e procedure appropriate che distinguano i compiti che svolge in qualità di organismo notificato dalle altre attività;

c) le necessarie procedure per svolgere le attività che tengono debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura, del grado di complessità della tecnologia del prodotto in questione e della natura di massa o seriale del processo produttivo.

L'organismo di valutazione della conformità dispone dei mezzi necessari per eseguire i compiti tecnici e amministrativi connessi alle attività di valutazione della conformità in modo appropriato e ha accesso a tutti gli strumenti o impianti occorrenti.

7. Il personale responsabile dell'esecuzione delle attività di valutazione della conformità dispone di quanto segue:

a) una formazione tecnica e professionale solida che includa tutte le attività di valutazione della conformità per cui l'organismo di valutazione della conformità è stato notificato;

b) soddisfacenti conoscenze dei requisiti relativi alle valutazioni che esegue e un'adeguata autorità per eseguire tali valutazioni;

c) una conoscenza e una comprensione adeguate dei requisiti essenziali di cibersicurezza di cui all'allegato I, delle norme armonizzate e delle specifiche comuni applicabili e delle disposizioni pertinenti della normativa di armonizzazione dell'Unione, nonché degli atti di esecuzione;

d) la capacità di redigere certificati, registri e relazioni atti a dimostrare che le valutazioni sono state eseguite.

8. È garantita l'imparzialità degli organismi di valutazione della conformità, dei loro alti dirigenti e del personale addetto alle valutazioni.

La remunerazione degli alti dirigenti e del personale addetto alle valutazioni di un organismo di valutazione della conformità non dipende dal numero di valutazioni eseguite o dai risultati di tali valutazioni.

9. Gli organismi di valutazione della conformità sottoscrivono un contratto di assicurazione per la responsabilità civile, a meno che detta responsabilità non sia direttamente coperta dal rispettivo Stato membro a norma del diritto nazionale o che lo Stato membro stesso non sia direttamente responsabile della valutazione della conformità.

10. Il personale dell'organismo di valutazione della conformità è tenuto al segreto professionale per tutto ciò di cui viene a conoscenza nell'esercizio delle sue funzioni a norma dell'allegato VIII o di qualsiasi disposizione esecutiva di diritto interno, tranne nei confronti delle autorità di vigilanza del mercato dello Stato membro in cui esercita le sue attività. Sono tutelati i diritti di proprietà. L'organismo di valutazione della conformità dispone di procedure documentate che garantiscono la conformità al presente paragrafo.

11. Gli organismi di valutazione della conformità partecipano alle attività di normazione pertinenti e alle attività del gruppo di coordinamento degli organismi notificati istituito a norma dell'articolo 51, o garantiscono che il loro personale addetto alle valutazioni ne sia informato, e applicano come guida generale le decisioni e i documenti amministrativi prodotti da tale gruppo.

12. Gli organismi di valutazione della conformità operano secondo modalità e condizioni coerenti, eque, proporzionate e ragionevoli, evitando nel contempo oneri inutili per gli operatori economici, tenendo conto in particolare degli interessi delle microimprese e delle piccole e medie imprese in relazione alle tariffe.

Articolo 40

Presunzione di conformità degli organismi notificati

Qualora dimostri la propria conformità ai criteri stabiliti nelle pertinenti norme armonizzate o in parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, un organismo di valutazione della conformità è considerato conforme ai requisiti di cui all'articolo 39 nella misura in cui le norme applicabili armonizzate contemplano tali requisiti.

Articolo 41

Affiliate e subappaltatori degli organismi notificati

1. L'organismo notificato, qualora subappalti compiti specifici connessi alla valutazione della conformità oppure ricorra a un'affiliata, garantisce che il subappaltatore o l'affiliata soddisfi i requisiti di cui all'articolo 39 e ne informa l'autorità di notifica.

2. L'organismo notificato si assume la completa responsabilità dei compiti eseguiti dai subappaltatori o dalle affiliate, ovunque siano stabiliti.

3. Le attività possono essere subappaltate o eseguite da un'affiliata solo con il consenso del fabbricante.

4. Gli organismi notificati tengono a disposizione dell'autorità di notifica i documenti pertinenti riguardanti la valutazione delle qualifiche del subappaltatore o dell'affiliata e il lavoro da essi eseguito a norma del presente regolamento.

Articolo 42

Domanda di notifica

1. L'organismo di valutazione della conformità presenta una domanda di notifica all'autorità di notifica dello Stato membro in cui è stabilito.

2. Tale domanda è corredata di una descrizione delle attività di valutazione della conformità, della procedura o delle procedure di valutazione della conformità e del prodotto o dei prodotti con elementi digitali per i quali l'organismo dichiara di essere competente, nonché, ove applicabile, di un certificato di accreditamento rilasciato da un organismo nazionale di accreditamento che attesti che l'organismo di valutazione della conformità è conforme ai requisiti di cui all'articolo 39.

3. Qualora l'organismo di valutazione della conformità non possa fornire un certificato di accreditamento, esso fornisce all'autorità di notifica tutte le prove documentali necessarie per la verifica, il riconoscimento e il controllo periodico della sua conformità ai requisiti di cui all'articolo 39.

Articolo 43

Procedura di notifica

1. Le autorità di notifica notificano solo gli organismi di valutazione della conformità che soddisfino i requisiti di cui all'articolo 39.

2. L'autorità di notifica informa la Commissione e gli altri Stati membri utilizzando il sistema informativo NANDO (*New Approach Notified and Designated Organisations*), sviluppato e gestito dalla Commissione.

3. La notifica include tutti i dettagli riguardanti le attività di valutazione della conformità, il modulo o i moduli di valutazione della conformità e il prodotto o i prodotti con elementi digitali interessati, nonché la relativa attestazione di competenza.

4. Qualora una notifica non sia basata su un certificato di accreditamento di cui all'articolo 42, paragrafo 2, l'autorità di notifica fornisce alla Commissione e agli altri Stati membri le prove documentali che attestino la competenza dell'organismo di valutazione della conformità nonché le disposizioni predisposte per fare in modo che tale organismo sia controllato periodicamente e continui a soddisfare i requisiti di cui all'articolo 39.

5. L'organismo interessato può eseguire le attività di un organismo notificato solo se non sono sollevate obiezioni da parte della Commissione o degli altri Stati membri entro due settimane dalla notifica, qualora sia usato un certificato di accreditamento, o entro due mesi dalla notifica qualora non sia usato un accreditamento.

Solo tale organismo è considerato un organismo notificato ai fini del presente regolamento.

6. Alla Commissione e agli altri Stati membri sono comunicate eventuali modifiche di rilievo riguardanti la notifica.

Articolo 44

Numeri di identificazione ed elenchi degli organismi notificati

1. La Commissione attribuisce un numero di identificazione a ciascun organismo notificato.

Essa assegna un numero unico anche se l'organismo è notificato a norma di diversi atti giuridici dell'Unione.

2. La Commissione mette a disposizione del pubblico l'elenco degli organismi notificati a norma del presente regolamento, inclusi i numeri di identificazione loro assegnati e le attività per le quali sono stati notificati.

La Commissione provvede affinché l'elenco sia tenuto aggiornato.

Articolo 45

Modifiche delle notifiche

1. Qualora accerti o sia informata che un organismo notificato non è più conforme ai requisiti di cui all'articolo 39, o non adempie ai suoi obblighi, l'autorità di notifica limita, sospende o ritira la notifica, a seconda dei casi, in funzione della gravità del mancato rispetto di tali requisiti o dell'inadempimento di tali obblighi. Essa ne informa immediatamente la Commissione e gli altri Stati membri.

2. In caso di limitazione, sospensione o ritiro della notifica, oppure di cessazione dell'attività dell'organismo notificato, lo Stato membro notificante adotta le misure appropriate per garantire che le pratiche di tale organismo siano evase da un altro organismo notificato o siano messe a disposizione delle autorità di notifica e di vigilanza del mercato responsabili, su loro richiesta.

Articolo 46

Contestazione della competenza degli organismi notificati

1. La Commissione indaga su tutti i casi in cui abbia dubbi o in cui siano portati alla sua attenzione dubbi sulla competenza di un organismo notificato a soddisfare i requisiti e ad adempiere le responsabilità cui è sottoposto o sulla continua ottemperanza di un organismo notificato a tali requisiti e a tali responsabilità.

2. Lo Stato membro notificante fornisce alla Commissione, su richiesta, tutte le informazioni relative alla base della notifica o del mantenimento della competenza dell'organismo in questione.

3. La Commissione garantisce la riservatezza di tutte le informazioni sensibili raccolte nel corso delle sue indagini.

4. La Commissione, qualora accerti che un organismo notificato non soddisfa o non soddisfa più i requisiti per la sua notifica, ne informa lo Stato membro notificante e chiede a quest'ultimo di adottare le misure correttive necessarie, incluso all'occorrenza il ritiro della notifica.

Articolo 47

Obblighi operativi degli organismi notificati

1. Gli organismi notificati eseguono le valutazioni della conformità conformemente alle procedure di valutazione della conformità di cui all'articolo 32 e all'allegato VIII.

2. Le valutazioni della conformità sono eseguite in modo proporzionato, evitando oneri inutili per gli operatori economici. Gli organismi di valutazione della conformità svolgono le loro attività tenendo debitamente conto delle dimensioni delle imprese, in particolare per quanto riguarda le microimprese e le piccole e medie imprese, del settore in cui operano, della loro struttura, del grado di complessità e del livello di rischio di cibersicurezza dei prodotti con elementi digitali e della tecnologia in questione e della natura di massa o seriale del processo produttivo.

3. Gli organismi notificati rispettano tuttavia il grado di rigore e il livello di tutela necessari per la conformità dei prodotti con elementi digitali al presente regolamento.

4. Se un organismo notificato accerta che un fabbricante non ha rispettato i requisiti di cui all'allegato I o alle corrispondenti norme armonizzate o specifiche comuni di cui all'articolo 27, chiede a tale fabbricante di adottare le misure correttive del caso e non rilascia un certificato di conformità.

5. Qualora nel corso del monitoraggio della conformità successivo al rilascio di un certificato un organismo notificato rilevi che un prodotto con elementi digitali non è più conforme ai requisiti stabiliti dal presente regolamento, esso chiede al fabbricante di adottare le misure correttive del caso e all'occorrenza sospende o ritira il certificato.

6. Qualora non siano adottate misure correttive o queste ultime non producano il risultato richiesto, l'organismo notificato limita, sospende o ritira i certificati, a seconda dei casi.

Articolo 48

Ricorso contro le decisioni degli organismi notificati

Gli Stati membri provvedono affinché sia disponibile una procedura di ricorso contro le decisioni degli organismi notificati.

Articolo 49

Obbligo di informazione a carico degli organismi notificati

1. Gli organismi notificati informano l'autorità di notifica:

a) di qualunque rifiuto, limitazione, sospensione o ritiro di un certificato;

b) di qualunque circostanza che possa influire sull'ambito e sulle condizioni della notifica;

c) di eventuali richieste di informazioni che abbiano ricevuto dalle autorità di vigilanza del mercato, in relazione ad attività di valutazione della conformità;

d) su richiesta, delle attività di valutazione della conformità eseguite nell'ambito della loro notifica e di qualsiasi altra attività svolta, incluse quelle transfrontaliere e relative al subappalto.

2. Gli organismi notificati forniscono agli altri organismi notificati a norma del presente regolamento, le cui attività di valutazione della conformità sono simili e hanno come oggetto gli stessi prodotti con elementi digitali, informazioni pertinenti su questioni relative ai risultati negativi e, su richiesta, ai risultati positivi delle valutazioni della conformità.

Articolo 50

Scambio di esperienze

La Commissione provvede all'organizzazione di uno scambio di esperienze tra le autorità nazionali degli Stati membri responsabili della politica di notifica.

Articolo 51

Coordinamento degli organismi notificati

1. La Commissione garantisce l'istituzione e il corretto funzionamento di un coordinamento e una cooperazione appropriati tra organismi notificati sotto forma di un gruppo intersettoriale di organismi notificati.

2. Gli Stati membri garantiscono che gli organismi da essi notificati partecipino al lavoro di tale gruppo, direttamente o mediante rappresentanti designati.

CAPO V

VIGILANZA DEL MERCATO E APPLICAZIONE DELLE NORME

Articolo 52

Vigilanza del mercato e controllo dei prodotti con elementi digitali nel mercato dell'Unione

1. Il regolamento (UE) 2019/1020 si applica ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento.

2. Ciascuno Stato membro designa una o più autorità di vigilanza del mercato al fine di garantire l'efficace attuazione del presente regolamento. Gli Stati membri possono designare un'autorità già esistente o una nuova autorità che agisca come autorità di vigilanza del mercato ai fini del presente regolamento.

3. Le autorità di vigilanza del mercato designate a norma del paragrafo 2 del presente articolo sono altresì responsabili dell'esecuzione delle attività di vigilanza del mercato in relazione agli obblighi per i gestori di software open source di cui all'articolo 24. Se un'autorità di vigilanza del mercato constata che un gestore di software open source non rispetta gli obblighi previsti in tale articolo, essa richiede al gestore di software open source di garantire che siano adottate tutte le opportune misure correttive. I gestori di software open source garantiscono che siano adottate tutte le opportune misure correttive in relazione agli obblighi loro spettanti in virtù del presente regolamento.

4. Le autorità di vigilanza del mercato collaborano, se pertinente, con le autorità nazionali di certificazione della cibersicurezza designate a norma dell'articolo 58 del regolamento (UE) 2019/881 e procedono regolarmente a scambi di informazioni. Per quanto riguarda la sorveglianza dell'attuazione degli obblighi di segnalazione di cui all'articolo 14 del presente regolamento, le autorità di vigilanza del mercato designate collaborano e procedono regolarmente a scambi di informazioni con i CSIRT designati come coordinatori e con l'ENISA.

5. Le autorità di vigilanza del mercato possono chiedere a un CSIRT designato come coordinatore e all'ENISA di fornire consulenza tecnica su questioni relative all'attuazione e all'applicazione del presente regolamento. Nel condurre un'indagine a norma dell'articolo 54, le autorità di vigilanza del mercato possono chiedere al CSIRT designato come coordinatore o all'ENISA di fornire un'analisi a sostegno delle valutazioni sulla conformità dei prodotti con elementi digitali.

6. Le autorità di vigilanza del mercato cooperano, se pertinente, con altre autorità di vigilanza del mercato designate sulla base di normative di armonizzazione dell'Unione diverse dal presente regolamento e procedono regolarmente a scambi di informazioni.

7. Le autorità di vigilanza del mercato collaborano, all'occorrenza, con le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati. Rientra in tale cooperazione la comunicazione a dette autorità di qualsiasi risultanza pertinente per l'esercizio delle loro competenze, anche nell'ambito della fornitura di orientamenti e consulenze a norma del paragrafo 10, se tali orientamenti e consulenze riguardano il trattamento dei dati personali.

Le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati hanno il potere di richiedere qualsiasi documentazione creata o conservata a norma del presente regolamento e di accedervi, qualora l'accesso a tale documentazione sia necessario per lo svolgimento dei loro compiti. Esse informano le autorità di vigilanza del mercato designate dello Stato membro interessato di tale richiesta.

8. Gli Stati membri garantiscono che le autorità di vigilanza del mercato designate dispongano di adeguate risorse finanziarie e tecniche, compresi, se del caso, strumenti per il trattamento automatizzato, nonché umane dotate delle competenze in materia di cibersicurezza necessarie per svolgere i loro compiti a norma del presente regolamento.

9. La Commissione incoraggia e agevola lo scambio di esperienze tra le autorità di vigilanza del mercato designate.

10. Le autorità di vigilanza del mercato possono fornire agli operatori economici orientamenti e consulenza sull'attuazione del presente regolamento, con il sostegno della Commissione e, se del caso, dei CSIRT e dell'ENISA.

11. Le autorità di vigilanza del mercato informano i consumatori riguardo a dove possono presentare reclami che potrebbero indicare una non conformità al presente regolamento, conformemente all'articolo 11 del regolamento (UE) 2019/1020, e forniscono ai consumatori informazioni su dove e come accedere ai meccanismi per facilitare la segnalazione di vulnerabilità, incidenti e minacce informatiche che possono incidere sui prodotti con elementi digitali.

12. Le autorità di vigilanza del mercato facilitano, ove pertinente, la cooperazione con i pertinenti portatori di interessi, comprese le organizzazioni scientifiche, di ricerca e di consumatori.

13. Le autorità di vigilanza del mercato riferiscono annualmente alla Commissione in merito ai risultati delle pertinenti attività di vigilanza del mercato. Le autorità di vigilanza del mercato designate comunicano senza indugio alla Commissione e alle pertinenti autorità nazionali garanti della concorrenza qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per l'applicazione del diritto dell'Unione in materia di concorrenza.

14. Per quanto riguarda i prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento classificati come sistemi di IA ad alto rischio a norma dell'articolo 6 del regolamento (UE) 2024/1689, le autorità di vigilanza del mercato designate ai fini di tale regolamento sono le autorità responsabili delle attività di vigilanza del mercato previste dal presente regolamento. Le autorità di vigilanza del mercato designate a norma del regolamento (UE) 2024/1689 cooperano, all'occorrenza, con le autorità di vigilanza del mercato designate a norma del presente regolamento e, per quanto riguarda la sorveglianza dell'attuazione degli obblighi di segnalazione a norma dell'articolo 14 del presente regolamento, con i CSIRT designati come coordinatori e con l'ENISA. Le autorità di vigilanza del mercato designate a norma del regolamento (UE) 2024/1689 informano in particolare le autorità di vigilanza del mercato designate a norma del presente regolamento di qualsiasi risultanza pertinente per lo svolgimento dei loro compiti in relazione all'attuazione del presente regolamento.

15. Per l'applicazione uniforme del presente regolamento è istituito un apposito gruppo di cooperazione amministrativa (ADCO) a norma dell'articolo 30, paragrafo 2, del regolamento (UE) 2019/1020. L'ADCO è composto da rappresentanti delle autorità di vigilanza del mercato designate e, se del caso, da rappresentanti degli uffici unici di collegamento. L'ADCO affronta inoltre questioni specifiche relative alle attività di vigilanza del mercato in relazione agli obblighi imposti ai gestori di software open source.

16. Le autorità di vigilanza del mercato monitorano il modo in cui i fabbricanti hanno applicato i criteri di cui all'articolo 13, paragrafo 8, nel determinare il periodo di assistenza dei loro prodotti con elementi digitali.

L'ADCO pubblica in una forma accessibile al pubblico e di facile utilizzo statistiche pertinenti sulle categorie di prodotti con elementi digitali, compreso i periodi medi di assistenza, quali determinati dal fabbricante a norma dell'articolo 13, paragrafo 8, e fornisce orientamenti che includano periodi di assistenza indicativi per le categorie di prodotti con elementi digitali.

Qualora i dati suggeriscano periodi di assistenza inadeguati per specifiche categorie di prodotti con elementi digitali, l'ADCO può formulare raccomandazioni alle autorità di vigilanza del mercato affinché concentrino le loro attività su tali categorie di prodotti con elementi digitali.

Articolo 53

Accesso ai dati e documentazione

Se necessario per valutare la conformità dei prodotti con elementi digitali e dei processi messi in atto dai loro fabbricanti ai requisiti essenziali di cibersicurezza di cui all'allegato I e su richiesta motivata, alle autorità di vigilanza del mercato è consentito l'accesso, in una lingua che esse siano in grado di comprendere facilmente, ai dati necessari per valutare la progettazione, lo sviluppo, la produzione e la gestione delle vulnerabilità di tali prodotti, compresa la relativa documentazione interna del pertinente operatore economico.

Articolo 54

Procedura a livello nazionale relativa ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo

1. Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia motivi sufficienti per ritenere che un prodotto con elementi digitali, compresa la relativa gestione delle vulnerabilità, presenti un rischio di cibersicurezza significativo, essa effettua, senza indebito ritardo e, se del caso, in cooperazione con il pertinente CSIRT, una valutazione del prodotto con elementi digitali interessato per quanto riguarda la sua conformità a tutti i requisiti di cui al presente regolamento. Gli operatori economici interessati cooperano con l'autorità di vigilanza del mercato se necessario.

Se, nel corso di tale valutazione, l'autorità di vigilanza del mercato conclude che il prodotto con elementi digitali non rispetta i requisiti di cui al presente regolamento, essa chiede senza indugio all'operatore economico interessato di adottare tutte le opportune misure correttive al fine di rendere il prodotto con elementi digitali conforme ai suddetti requisiti oppure di ritirarlo o di richiamarlo dal mercato entro un termine ragionevole e proporzionato alla natura del rischio di cibersicurezza, a seconda di quanto prescritto dall'autorità di vigilanza del mercato.

L'autorità di vigilanza del mercato informa di conseguenza l'organismo notificato pertinente. L'articolo 18 del regolamento (UE) 2019/1020 si applica alle misure correttive.

2. Nel determinare la rilevanza di un rischio di cibersicurezza di cui al paragrafo 1 del presente articolo, le autorità di vigilanza del mercato tengono conto anche dei fattori di rischio non tecnici, in particolare quelli stabiliti a seguito di valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22 della direttiva (UE) 2022/2555. Se l'autorità di vigilanza del mercato ha motivi sufficienti per ritenere che un prodotto con elementi digitali presenti un rischio di cibersicurezza significativo alla luce di fattori di rischio non tecnici, essa informa le autorità competenti designate o istituite a norma dell'articolo 8 della direttiva (UE) 2022/2555 e coopera con tali autorità se necessario.

3. Qualora ritenga che la non conformità non sia limitata al territorio nazionale, l'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri dei risultati della valutazione e delle azioni che ha chiesto all'operatore economico di intraprendere.

4. L'operatore economico garantisce che siano adottate tutte le opportune misure correttive nei confronti di tutti i prodotti con elementi digitali interessati che ha messo a disposizione sul mercato in tutta l'Unione.

5. Qualora l'operatore economico non adotti misure correttive adeguate entro il termine di cui al paragrafo 1, secondo comma, l'autorità di vigilanza del mercato adotta tutte le opportune misure provvisorie per vietare o limitare la messa a disposizione del prodotto con elementi digitali sul suo mercato nazionale, per ritirarlo da tale mercato o per richiamarlo.

Tale autorità notifica senza indugio alla Commissione e agli altri Stati membri tali misure.

6. Le informazioni di cui al paragrafo 5 includono tutti i dettagli disponibili, soprattutto i dati necessari all'identificazione del prodotto con elementi digitali non conforme, la sua origine, la natura della presunta non conformità e i rischi connessi, la natura e la durata delle misure nazionali adottate, nonché gli argomenti espressi dall'operatore economico interessato. L'autorità di vigilanza del mercato indica in particolare se la non conformità sia dovuta a una o più delle cause seguenti:

a) mancato rispetto dei requisiti essenziali di cibersicurezza di cui all'allegato I da parte del prodotto con elementi digitali o dei processi messi in atto dal fabbricante;

b) carenze nelle norme armonizzate, nei sistemi europei di certificazione della cibersicurezza o nelle specifiche comuni di cui all'articolo 27.

7. Le autorità di vigilanza del mercato degli Stati membri diverse dall'autorità di vigilanza del mercato dello Stato membro che ha avviato la procedura comunicano senza indugio alla Commissione e agli altri Stati membri tutte le misure adottate, tutte le altre informazioni a loro disposizione sulla non conformità del prodotto con elementi digitali interessato e, in caso di disaccordo con la misura nazionale notificata, le loro obiezioni.

8. Qualora, entro tre mesi dal ricevimento della notifica di cui al paragrafo 5 del presente articolo, uno Stato membro o la Commissione non sollevino obiezioni contro la misura provvisoria adottata da uno Stato membro, tale misura è considerata giustificata. Ciò non pregiudica i diritti procedurali dell'operatore economico interessato in conformità dell'articolo 18 del regolamento (UE) 2019/1020.

9. Le autorità di vigilanza del mercato di tutti gli Stati membri garantiscono che siano adottate senza indugio adeguate misure restrittive in relazione al prodotto con elementi digitali interessato, come il ritiro di tale prodotto dal loro mercato.

Articolo 55

Procedura di salvaguardia dell'Unione

1. Se entro tre mesi dal ricevimento della notifica di cui all'articolo 54, paragrafo 5, uno Stato membro solleva obiezioni contro la misura adottata da un altro Stato membro, o se la Commissione ritiene che la misura sia contraria al diritto dell'Unione, la Commissione consulta senza indugio lo Stato membro interessato e l'operatore o gli operatori economici e valuta la misura nazionale. Sulla base dei risultati di tale valutazione, la Commissione decide se la misura nazionale sia giustificata o meno entro nove mesi dalla notifica di cui all'articolo 54, paragrafo 5, e notifica tale decisione allo Stato membro interessato.

2. Se la misura nazionale è considerata giustificata, tutti gli Stati membri adottano le misure necessarie a garantire che il prodotto con elementi digitali non conforme sia ritirato dal loro mercato e ne informano la Commissione. Se la misura nazionale non è considerata giustificata, lo Stato membro interessato provvede a ritirarla.

3. Se la misura nazionale è considerata giustificata e la non conformità del prodotto con elementi digitali è attribuita a carenze nelle norme armonizzate, la Commissione applica la procedura di cui all'articolo 11 del regolamento (UE) n. 1025/2012.

4. Se la misura nazionale è considerata giustificata e la non conformità del prodotto con elementi digitali è attribuita a carenze in un sistema europeo di certificazione della cibersicurezza di cui all'articolo 27, la Commissione valuta se modificare o abrogare qualsiasi atto delegato adottato conformemente all'articolo 27, paragrafo 9, che specifica la presunzione di conformità relativa a tale sistema di certificazione.

5. Se la misura nazionale è considerata giustificata e la non conformità del prodotto con elementi digitali è attribuita a carenze nelle specifiche comuni di cui all'articolo 27, la Commissione valuta se modificare o abrogare qualsiasi atto delegato adottato a norma dell'articolo 27, paragrafo 2, che stabilisce tali specifiche comuni.

Articolo 56

Procedura a livello di Unione relativa ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo

1. Se la Commissione ha motivi sufficienti per ritenere, anche sulla base delle informazioni fornite dall'ENISA, che un prodotto con elementi digitali che presenta un rischio di cibersicurezza significativo non sia conforme ai requisiti stabiliti nel presente regolamento, ne informa le autorità di vigilanza del mercato. Se le autorità di vigilanza del mercato effettuano una valutazione di tale prodotto con elementi digitali che può presentare un rischio di cibersicurezza significativo per quanto riguarda la sua conformità ai requisiti di cui al presente regolamento, si applicano le procedure di cui agli articoli 54 e 55.

2. Se la Commissione ha motivi sufficienti per ritenere che un prodotto con elementi digitali presenti un rischio di cibersicurezza significativo alla luce di fattori di rischio non tecnici, essa informa le autorità di vigilanza del mercato competenti e, se del caso, le autorità competenti designate o istituite ai sensi dell'articolo 8 della direttiva (UE) 2022/2555 e coopera con tali autorità se necessario. La Commissione valuta inoltre la pertinenza dei rischi individuati per tale prodotto con elementi digitali alla luce dei suoi compiti per quanto riguarda le valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche di cui all'articolo 22 della direttiva (UE) 2022/2555 e consulta, se necessario, il gruppo di cooperazione istituito a norma dell'articolo 14 della direttiva (UE) 2022/2555 e l'ENISA.

3. In circostanze che giustifichino un intervento immediato per preservare il corretto funzionamento del mercato interno e qualora la Commissione abbia motivi sufficienti per ritenere che il prodotto con elementi digitali di cui al paragrafo 1 continui a non essere conforme ai requisiti stabiliti dal presente regolamento e che non siano state adottate misure efficaci dalle autorità di vigilanza del mercato competenti, la Commissione effettua una valutazione della conformità e può chiedere all'ENISA di fornire un'analisi a sostegno di tale valutazione. La Commissione ne informa le autorità di vigilanza del mercato pertinenti. Gli operatori economici interessati cooperano con l'ENISA se necessario.

4. Sulla base della valutazione di cui al paragrafo 3, la Commissione può decidere che è necessaria una misura correttiva o restrittiva a livello dell'Unione. A tal fine essa consulta senza indugio gli Stati membri interessati e l'operatore o gli operatori economici interessati.

5. Sulla base della consultazione di cui al paragrafo 4 del presente articolo, la Commissione può adottare atti di esecuzione per prevedere misure correttive o restrittive a livello dell'Unione, tra cui imporre di ritirare dal mercato i prodotti con elementi digitali interessati o di richiamarli, entro un termine ragionevole, proporzionato alla natura del rischio. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

6. La Commissione comunica immediatamente gli atti di esecuzione di cui al paragrafo 5 all'operatore o agli operatori economici interessati. Gli Stati membri attuano senza indugio tali atti di esecuzione e ne informano la Commissione.

7. I paragrafi da 3 a 6 si applicano per la durata della situazione eccezionale che ha giustificato l'intervento della Commissione, purché il prodotto con elementi digitali in questione non sia reso conforme al presente regolamento.

Articolo 57

Prodotti con elementi digitali conformi che presentano un rischio di cibersicurezza significativo

1. L'autorità di vigilanza del mercato di uno Stato membro chiede a un operatore economico di adottare tutte le misure del caso qualora, dopo aver effettuato una valutazione ai sensi dell'articolo 54, ritenga che, sebbene conformi al presente regolamento, il prodotto con elementi digitali e i processi messi in atto dal fabbricante presentino un rischio di cibersicurezza significativo e comportino inoltre un rischio per:

a) la salute o la sicurezza delle persone;

b) la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali;

c) la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti utilizzando un sistema di informazione elettronico da parte di soggetti essenziali del tipo di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555; o

d) altri aspetti della tutela dell'interesse pubblico.

Le misure di cui al primo comma possono includere misure appropriate a far sì che il prodotto con elementi digitali e i processi messi in atto dal fabbricante non presentino più i rischi in questione all'atto della messa a disposizione sul mercato oppure che il prodotto con elementi digitali in questione sia ritirato dal mercato o richiamato, e sono commisurate alla natura di tali rischi.

2. Il fabbricante o altri operatori economici pertinenti garantiscono l'adozione di misure correttive nei confronti dei prodotti con elementi digitali interessati che hanno messo a disposizione sul mercato in tutta l'Unione entro il termine stabilito dall'autorità di vigilanza del mercato dello Stato membro di cui al paragrafo 1.

3. Lo Stato membro informa immediatamente la Commissione e gli altri Stati membri in merito alle misure adottate a norma del paragrafo 1. Tali informazioni comprendono tutti i dettagli disponibili, segnatamente i dati necessari all'identificazione dei prodotti con elementi digitali interessati, l'origine e la catena di approvvigionamento di tali prodotti, la natura dei rischi connessi, nonché la natura e la durata delle misure nazionali adottate.

4. La Commissione avvia senza indugio consultazioni con gli Stati membri e l'operatore economico interessato e valuta le misure nazionali adottate. In base ai risultati della valutazione, la Commissione decide se la misura sia giustificata o no e propone, all'occorrenza, misure appropriate.

5. La Commissione trasmette la decisione di cui al paragrafo 4 agli Stati membri.

6. Se ha motivi sufficienti per ritenere, anche sulla base delle informazioni fornite dall'ENISA, che un prodotto con elementi digitali, sebbene conforme al presente regolamento, presenti i rischi di cui al paragrafo 1 del presente articolo, la Commissione ne dà informazione e può chiedere all'autorità o alle autorità di vigilanza del mercato competenti di effettuare una valutazione e di seguire le procedure di cui all'articolo 54 e ai paragrafi 1, 2 e 3 del presente articolo.

7. In circostanze che giustifichino un intervento immediato per preservare il corretto funzionamento del mercato interno e qualora la Commissione abbia motivi sufficienti per ritenere che il prodotto con elementi digitali di cui al paragrafo 6 continui a presentare i rischi di cui al paragrafo 1 e che le autorità nazionali di vigilanza del mercato competenti non abbiano adottato misure efficaci, la Commissione effettua una valutazione dei rischi presentati da tale prodotto con elementi digitali e può chiedere all'ENISA di fornire un'analisi a sostegno di tale valutazione e ne informa le autorità di vigilanza del mercato competenti. Gli operatori economici interessati cooperano con l'ENISA se necessario.

8. Sulla base della valutazione di cui al paragrafo 7, la Commissione può stabilire che è necessaria una misura correttiva o restrittiva a livello dell'Unione. A tal fine essa consulta senza indugio gli Stati membri interessati e l'operatore o gli operatori economici interessati.

9. Sulla base della consultazione di cui al paragrafo 8 del presente articolo, la Commissione può adottare atti di esecuzione per decidere in merito alle misure correttive o restrittive a livello dell'Unione, tra cui imporre di ritirare dal mercato o di richiamare i prodotti con elementi digitali interessati, entro un termine ragionevole, proporzionato alla natura del rischio. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

10. La Commissione comunica immediatamente gli atti di esecuzione di cui al paragrafo 9 all'operatore o agli operatori economici interessati. Gli Stati membri attuano tali atti di esecuzione senza indugio e ne informano la Commissione.

11. I paragrafi da 6 a 10 si applicano per la durata della situazione eccezionale che ha giustificato l'intervento della Commissione e per tutto il tempo in cui il prodotto con elementi digitali in questione continua a presentare i rischi di cui al paragrafo 1.

Articolo 58

Non conformità formale

1. Un'autorità di vigilanza del mercato di uno Stato membro chiede al fabbricante interessato di porre fine alla non conformità contestata qualora giunga ad una delle conclusioni seguenti:

a) la marcatura CE è stata apposta in violazione dell'articolo 29 o dell'articolo 30;

b) la marcatura CE non è stata apposta;

c) la dichiarazione di conformità UE non è stata redatta;

d) la dichiarazione di conformità UE non è stata redatta correttamente;

e) il numero di identificazione dell'organismo notificato coinvolto nella procedura di valutazione della conformità, ove applicabile, non è stato apposto;

f) la documentazione tecnica non è disponibile o non è completa.

2. Se la non conformità di cui al paragrafo 1 permane, lo Stato membro interessato adotta tutte le misure appropriate per limitare o proibire la messa a disposizione sul mercato del prodotto con elementi digitali o per garantire che sia richiamato o ritirato dal mercato.

Articolo 59

Attività congiunte delle autorità di vigilanza del mercato

1. Le autorità di vigilanza del mercato possono stipulare accordi con altre autorità competenti per la realizzazione di attività congiunte volte a garantire la cibersicurezza e la tutela dei consumatori in relazione a specifici prodotti con elementi digitali immessi sul mercato o messi a disposizione sul mercato, in particolare i prodotti con elementi digitali che spesso presentano rischi di cibersicurezza.

2. La Commissione o l'ENISA propongono attività congiunte di verifica della conformità al presente regolamento che saranno svolte dalle autorità di vigilanza del mercato sulla base di indicazioni o informazioni riguardanti la potenziale non conformità, in diversi Stati membri, di prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento ai requisiti stabiliti da quest'ultimo.

3. Le autorità di vigilanza del mercato e, se del caso, la Commissione garantiscono che l'accordo sullo svolgimento di attività congiunte non comporti una concorrenza sleale tra gli operatori economici e non pregiudichi l'obiettività, l'indipendenza e l'imparzialità delle parti dell'accordo.

4. Un'autorità di vigilanza del mercato ha facoltà di utilizzare qualsivoglia informazione ottenuta come risultato delle attività congiunte svolte nell'ambito di un'indagine da essa condotta.

5. L'autorità di vigilanza del mercato competente e, se del caso, la Commissione mettono a disposizione del pubblico l'accordo sulle attività congiunte, compresi i nomi delle parti coinvolte.

Articolo 60

Indagini a tappeto

1. Le autorità di vigilanza del mercato conducono simultaneamente azioni di controllo coordinate (indagini a tappeto) di particolari prodotti con elementi digitali o relative categorie per verificarne la conformità con il presente regolamento o per individuare violazioni. Tali indagini a tappeto possono comprendere ispezioni di prodotti con elementi digitali acquistati sotto un'identità di copertura.

2. Salvo diverso accordo tra le autorità di vigilanza del mercato coinvolte, le indagini a tappeto sono coordinate dalla Commissione. Il coordinatore dell'indagine a tappeto mette a disposizione del pubblico, se del caso, i risultati aggregati.

3. L'ENISA, qualora nell'esecuzione dei suoi compiti, anche sulla base delle notifiche ricevute conformemente all'articolo 14, paragrafi 1 e 3, identifichi categorie di prodotti con elementi digitali per le quali possono essere organizzate indagini a tappeto, presenta una proposta per un'indagine a tappeto al coordinatore di cui al paragrafo 2 del presente articolo affinché sia esaminata dalle autorità di vigilanza del mercato.

4. Nello svolgere indagini a tappeto, le autorità di vigilanza del mercato coinvolte possono usare i poteri di indagine di cui agli articoli da 52 a 58 e gli altri poteri a esse conferiti dal diritto nazionale.

5. Le autorità di vigilanza del mercato possono invitare i funzionari della Commissione e altre persone di accompagnamento autorizzate dalla Commissione a partecipare alle indagini a tappeto.

CAPO VI

DELEGA DI POTERE E PROCEDURA DI COMITATO

Articolo 61

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 2, paragrafo 5, secondo comma, all'articolo 7, paragrafo 3, all'articolo 8, paragrafi 1 e 2, all'articolo 13, paragrafo 8, quarto comma, all'articolo 14, paragrafo 9, all'articolo 25, all'articolo 27, paragrafo 9, all'articolo 28, paragrafo 5, e all'articolo 31, paragrafo 5, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 10 dicembre 2024. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 2, paragrafo 5, secondo comma, all'articolo 7, paragrafo 3, all'articolo 8, paragrafi 1 e 2, all'articolo 13, paragrafo 8, quarto comma, all'articolo 14, paragrafo 9, all'articolo 25, all'articolo 27, paragrafo 9, all'articolo 28, paragrafo 5, e all'articolo 31, paragrafo 5, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 2, paragrafo 5, secondo comma, dell'articolo 7, paragrafo 3, dell'articolo 8, paragrafi 1 e 2, dell'articolo 13, paragrafo 8, quarto comma, dell'articolo 14, paragrafo 9, dell'articolo 25, dell'articolo 27, paragrafo 9, dell'articolo 28, paragrafo 5, o dell'articolo 31, paragrafo 5, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 62

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

3. Laddove il parere del comitato debba essere ottenuto con procedura scritta, questa procedura si conclude senza esito quando, entro il termine per la formulazione del parere, il presidente del comitato decida in tal senso o un membro del comitato lo richieda.

CAPO VII

RISERVATEZZA E SANZIONI

Articolo 63

Riservatezza

1. Tutte le parti che partecipano all'applicazione del presente regolamento rispettano la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, in particolare:

a) i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica, compreso il codice sorgente, tranne i casi cui si applica l'articolo 5 della direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio ([37]);

b) l'efficace attuazione del presente regolamento, in particolare per quanto riguarda ispezioni, indagini o audit;

c) gli interessi di sicurezza pubblica e nazionale;

d) l'integrità del procedimento penale o amministrativo.

2. Fatto salvo il paragrafo 1, le informazioni scambiate in via riservata tra le autorità di vigilanza del mercato e tra queste ultime e la Commissione non sono divulgate senza il preventivo accordo dell'autorità di vigilanza del mercato dalla quale tali informazioni provengono.

3. I paragrafi 1 e 2 non pregiudicano i diritti e gli obblighi della Commissione, degli Stati membri e degli organismi notificati in materia di scambio delle informazioni e di diffusione degli avvisi di sicurezza, né gli obblighi delle persone interessate di fornire informazioni a norma del diritto penale degli Stati membri.

4. La Commissione e gli Stati membri possono scambiare, ove necessario, informazioni sensibili con le autorità competenti dei paesi terzi con i quali abbiano concluso accordi di riservatezza, bilaterali o multilaterali, che garantiscano un livello di protezione adeguato.

Articolo 64

Sanzioni

1. Gli Stati membri fissano le norme sulle sanzioni applicabili in caso di violazione del presente regolamento e prendono tutti i provvedimenti necessari per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano tali norme e misure alla Commissione, senza indugio, e provvedono poi a dare immediata notifica delle eventuali modifiche successive.

2. La non conformità ai requisiti essenziali di cibersicurezza di cui all'allegato I e agli obblighi di cui agli articoli 13 e 14 è soggetta a sanzioni amministrative pecuniarie fino a 15 000 000 EUR o, se l'autore del reato è un'impresa, fino al 2,5 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

3. La non conformità agli obblighi di cui agli articoli da 18 a 23, all'articolo 28, all'articolo 30, paragrafi da 1 a 4, all'articolo 31, paragrafi da 1 a 4, all'articolo 32, paragrafi 1, 2 e 3, all'articolo 33, paragrafo 5, e agli articoli 39, 41, 47, 49 e 53 è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR o, se l'autore del reato è un'impresa, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

4. La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità di vigilanza del mercato è soggetta a sanzioni amministrative pecuniarie fino a 5 000 000 EUR o, se l'autore del reato è un'impresa, fino all'1 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

([37]) Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti (GU L 157 del 15.6.2016, pag. 1).

5. Nel decidere l'importo della sanzione amministrativa pecuniaria in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e si tiene quanto segue in debita considerazione:

a) la natura, la gravità e la durata della violazione e delle sue conseguenze;

b) se le stesse o altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore economico per una violazione analoga;

c) le dimensioni, in particolare per quanto riguarda le microimprese e le piccole e medie imprese, start up comprese, e la quota di mercato dell'operatore economico che ha commesso la violazione.

6. Le autorità di vigilanza del mercato che applicano sanzioni amministrative pecuniarie danno comunicazione di tale applicazione alle autorità di vigilanza del mercato di altri Stati membri mediante il sistema di informazione e comunicazione di cui all'articolo 34 del regolamento (UE) 2019/1020.

7. Ciascuno Stato membro può prevedere regole che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. A seconda dell'ordinamento giuridico degli Stati membri, le regole in materia di sanzioni amministrative pecuniarie possono essere applicate in modo tale che le sanzioni pecuniarie siano inflitte dai tribunali nazionali competenti o da altri organismi in base alle competenze stabilite a livello nazionale in tali Stati membri. L'applicazione di tali regole in tali Stati membri ha effetto equivalente.

9. Le sanzioni amministrative pecuniarie possono essere inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta a qualsiasi altra misura correttiva o restrittiva applicata dalle autorità di vigilanza del mercato per la stessa violazione.

10. In deroga ai paragrafi da 3 a 9, le sanzioni amministrative pecuniarie di cui a tali paragrafi non si applicano:

a) ai fabbricanti che si qualificano come microimprese o piccole imprese per quanto riguarda il mancato rispetto del termine di cui all'articolo 14, paragrafo 2, lettera a), o all'articolo 14, paragrafo 4, lettera a);

b) alle violazioni del presente regolamento da parte di gestori di software open-source.

Articolo 65

Azioni rappresentative

La direttiva (UE) 2020/1828 si applica alle azioni rappresentative intentate contro violazioni, da parte degli operatori economici, delle disposizioni del presente regolamento che ledono o possono ledere gli interessi collettivi dei consumatori.

CAPO VIII

DISPOSIZIONI TRANSITORIE E FINALI

Articolo 66

Modifica del regolamento (UE) 2019/1020

Nell'allegato I del regolamento (UE) 2019/1020 è aggiunto il punto seguente:

«72 Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio (*).

(*) Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (legge sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj)».

Articolo 67

Modifica della direttiva (UE) 2020/1828

Nell'allegato I della direttiva (UE) 2020/1828 è aggiunto il punto seguente:

«67 Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio (*).

(*) Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (legge sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj)».

Articolo 68

Modifica del regolamento (UE) n. 168/2013

All'allegato II, parte C1, del regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio ([38]), nella tabella è aggiunta la voce seguente:

«

16	18	protezione del veicolo dagli attacchi informatici		x	x	x	x	x	x	x	x	x	x	x	x	x	X

»

Articolo 69

Disposizioni transitorie

1. I certificati di esame UE del tipo e le decisioni di approvazione rilasciati in relazione ai requisiti di cibersicurezza per i prodotti con elementi digitali soggetti ad altra normativa di armonizzazione dell'Unione diversa dal presente regolamento rimangono validi fino all'11 giugno 2028, a meno che non scadano prima di tale data o non sia altrimenti disposto in tali altre normative di armonizzazione dell'Unione, nel qual caso rimangono validi come indicato in tali normative.

2. I prodotti con elementi digitali immessi sul mercato prima dell'11 dicembre 2027 sono soggetti ai requisiti stabiliti nel presente regolamento solo se, a decorrere da tale data, tali prodotti sono soggetti a una modifica sostanziale.

3. In deroga al paragrafo 2 del presente articolo, gli obblighi di cui all'articolo 14 si applicano a tutti i prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento e che sono stati immessi sul mercato prima dell'11 dicembre 2027.

Articolo 70

Valutazione e riesame

1. Entro l'11 dicembre 2030 e successivamente ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione sulla valutazione e sul riesame del presente regolamento. Tale relazione è pubblicata.

2. Entro l'11 settembre 2028, la Commissione, previa consultazione dell'ENISA e della rete di CSIRT, presenta al Parlamento europeo e al Consiglio una relazione in cui valuta l'efficacia della piattaforma unica di segnalazione indicata all'articolo 16, nonché l'impatto dell'applicazione dei motivi connessi alla cibersicurezza di cui all'articolo 16, paragrafo 2, da parte dei CSIRT designati come coordinatori sull'efficacia della piattaforma unica di segnalazione per quanto riguarda la diffusione tempestiva delle notifiche ricevute ad altri CSIRT pertinenti.

Articolo 71

Entrata in vigore e applicazione

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

([38]) Regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio, del 15 gennaio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore a due o tre ruote e dei quadricicli (GU L 60 del 2.3.2013, pag. 52).

2. Il presente regolamento si applica dall'11 dicembre 2027.

Tuttavia, l'articolo 14 si applica a decorrere dall'11 settembre 2026 e il capo IV (articoli da 35 a 51) si applica a decorrere dall'11 giugno 2026.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri

Fatto a Strasburgo, il 23 ottobre 2024

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	ZSIGMOND B. P.

ALLEGATO I

REQUISITI ESSENZIALI DI CIBERSICUREZZA

Parte I Requisiti di cibersicurezza relativi alle proprietà dei prodotti con elementi digitali

1) I prodotti con elementi digitali sono progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cibersicurezza in base ai rischi.

2) Sulla base della valutazione dei rischi di cibersicurezza di cui all'articolo 13, paragrafo 2, e ove applicabile, i prodotti con elementi digitali:

   a) sono messi a disposizione sul mercato senza vulnerabilità sfruttabili note;

   b) sono messi a disposizione sul mercato con una configurazione sicura per impostazione predefinita, salvo diverso accordo tra il fabbricante e l'utilizzatore commerciale in relazione a un prodotto su misura con elementi digitali, con la possibilità di ripristinare il prodotto allo stato originale;

   c) garantiscono che le vulnerabilità possano essere affrontate mediante aggiornamenti di sicurezza, anche, se del caso, mediante aggiornamenti di sicurezza automatici installati entro un periodo di tempo adeguato, abilitato come impostazione predefinita, con un meccanismo di disattivazione chiaro e di facile utilizzo, attraverso la notifica agli utilizzatori degli aggiornamenti disponibili e la possibilità di rinviarli temporaneamente;

   d) garantiscono la protezione dall'accesso non autorizzato mediante adeguati meccanismi di controllo, tra cui, a titolo esemplificativo ma non esaustivo, sistemi di autenticazione e di gestione dell'identità o dell'accesso, e segnalano eventuali accessi non autorizzati;

   e) proteggono la riservatezza dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, ad esempio criptando i pertinenti dati a riposo o in transito mediante meccanismi all'avanguardia, e utilizzando altri mezzi tecnici;

   f) proteggono l'integrità dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, dei comandi, dei programmi e della configurazione da qualsiasi manipolazione o modifica non autorizzata da parte dell'utilizzatore, e segnalano le corruzioni;

   g) trattano solo dati, personali o di altro tipo, adeguati, pertinenti e limitati a quanto necessario in relazione alla finalità prevista del prodotto con elementi digitali («minimizzazione dei dati»);

   h) proteggono la disponibilità delle funzioni essenziali e di base, anche dopo un incidente, anche attraverso misure di resilienza e di attenuazione contro gli attacchi di negazione del servizio (*denial of service*);

   i) riducono al minimo l'impatto negativo dei prodotti stessi o dei dispositivi connessi sulla disponibilità dei servizi forniti da altri dispositivi o reti;

   j) sono progettati, sviluppati e prodotti per limitare le superfici di attacco, comprese le interfacce esterne;

   k) sono progettati, sviluppati e prodotti per ridurre l'impatto degli incidenti utilizzando meccanismi e tecniche di attenuazione dello sfruttamento adeguati;

   l) forniscono informazioni sulla sicurezza registrando e monitorando le attività interne pertinenti, compresi l'accesso a dati, servizi o funzioni o la modifica degli stessi, con un meccanismo di disattivazione per l'utilizzatore;

   m) offrono agli utenti la possibilità di rimuovere in modo sicuro e agevole, su base permanente, tutti i dati e tutte le impostazioni e, qualora tali dati possano essere trasferiti ad altri prodotti o sistemi, garantiscono che ciò avvenga in modo sicuro.

Parte II Requisiti di gestione delle vulnerabilità

I fabbricanti di prodotti con elementi digitali:

1) identificano e documentano le vulnerabilità e i componenti contenuti nel prodotto con elementi digitali, redigendo anche una distinta base del software in un formato di uso comune e leggibile da un dispositivo automatico, che includa almeno le dipendenze di primo livello del prodotto;

2) in relazione ai rischi posti dai prodotti con elementi digitali, affrontano e correggono tempestivamente le vulnerabilità, anche fornendo aggiornamenti di sicurezza; ove tecnicamente fattibile, nuovi aggiornamenti di sicurezza sono forniti separatamente dagli aggiornamenti della funzionalità;

3) effettuano prove e riesami efficaci e periodici della sicurezza del prodotto con elementi digitali;

4) una volta reso disponibile un aggiornamento di sicurezza, condividono e divulgano pubblicamente informazioni sulle vulnerabilità risolte, compresi una descrizione delle vulnerabilità, informazioni che consentano agli utilizzatori di identificare il prodotto con elementi digitali interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni chiare e accessibili che aiutino gli utilizzatori a correggere le vulnerabilità; in casi debitamente giustificati, qualora ritengano che i rischi di sicurezza legati alla divulgazione siano superiori ai benefici in termini di sicurezza, i fabbricanti possono ritardare la divulgazione di informazioni su una vulnerabilità risolta fino a quando gli utilizzatori non abbiano avuto la possibilità di applicare la pertinente patch;

5) mettono in atto e applicano una politica di divulgazione coordinata delle vulnerabilità;

6) adottano misure per facilitare la condivisione di informazioni sulle potenziali vulnerabilità nel loro prodotto con elementi digitali e nei componenti di terzi contenuti in tale prodotto, fornendo anche un indirizzo di contatto per la segnalazione delle vulnerabilità individuate nel prodotto con elementi digitali;

7) prevedono meccanismi per distribuire in modo sicuro gli aggiornamenti dei prodotti con elementi digitali, per garantire che le vulnerabilità siano corrette o attenuate in modo tempestivo e, ove applicabile per gli aggiornamenti di sicurezza, in modo automatico;

8) garantiscono che, qualora disponibili, siano diffusi tempestivamente e gratuitamente, salvo diversamente convenuto tra un fabbricante e un utilizzatore commerciale in relazione a un prodotto su misura con elementi digitali, aggiornamenti di sicurezza per risolvere i problemi di sicurezza individuati, accompagnati da messaggi di avviso che forniscano agli utilizzatori le informazioni pertinenti, comprese le potenziali misure da adottare.

ALLEGATO II

INFORMAZIONI E ISTRUZIONI PER L'UTILIZZATORE

Il prodotto con elementi digitali è accompagnato, come minimo, dagli elementi seguenti:

1. il nome, la denominazione commerciale registrata o il marchio registrato del fabbricante e l'indirizzo postale, l'indirizzo di posta elettronica o altro contatto digitale nonché, ove disponibile, il sito web a cui il fabbricante può essere contattato;
2. il punto di contatto unico dove è possibile segnalare e ricevere informazioni sulle vulnerabilità del prodotto con elementi digitali e dove è possibile trovare la politica del fabbricante sulla divulgazione coordinata delle vulnerabilità;
3. nome e tipo e qualsiasi altra informazione che consenta l'identificazione univoca del prodotto con elementi digitali;
4. la finalità prevista del prodotto con elementi digitali, compreso l'ambiente di sicurezza fornito dal fabbricante, nonché le funzionalità essenziali del prodotto e le informazioni sulle proprietà di sicurezza;
5. qualsiasi circostanza nota o prevedibile connessa all'uso del prodotto con elementi digitali in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi di cibersicurezza significativi;
6. se del caso, l'indirizzo Internet dove è possibile accedere alla dichiarazione di conformità UE;
7. il tipo di assistenza tecnica di sicurezza offerta dal fabbricante e la data finale del periodo di assistenza durante il quale gli utilizzatori possono aspettarsi che le vulnerabilità siano gestite e di ricevere gli aggiornamenti di sicurezza;
8. istruzioni dettagliate o un indirizzo Internet che rimandi a tali istruzioni e informazioni su quanto segue:
   a) le misure necessarie durante la prima messa in servizio e per tutta la durata del prodotto con elementi digitali per garantirne l'uso sicuro;
   b) in che modo le modifiche del prodotto con elementi digitali possono influire sulla sicurezza dei dati;
   c) le modalità di installazione degli aggiornamenti rilevanti per la sicurezza;
   d) lo smantellamento sicuro del prodotto con elementi digitali, comprese le informazioni sulle modalità di eliminazione sicura dei dati degli utilizzatori
   e) come può essere disattivata l'impostazione predefinita che consente l'installazione automatica degli aggiornamenti di sicurezza, come richiesto nell'allegato I, parte I, punto 2, lettera c);
   f) se il prodotto con elementi digitali è destinato all'integrazione in altri prodotti con elementi digitali, le informazioni necessarie affinché l'integratore soddisfi i requisiti essenziali di cibersicurezza di cui all'allegato I e i requisiti di documentazione di cui all'allegato VII.
9. Se il fabbricante decide di mettere a disposizione dell'utilizzatore la distinta base del software, informazioni sul luogo in cui è possibile accedere a tale distinta.

ALLEGATO III

PRODOTTI CON ELEMENTI DIGITALI IMPORTANTI

Classe I

1. Sistemi di gestione dell'identità e software e hardware per la gestione degli accessi privilegiati, compresi i lettori di autenticazione e controllo degli accessi, tra cui i lettori biometrici
2. browser autonomi e incorporati
3. sistemi di gestione delle password
4. software che cercano, rimuovono o mettono in quarantena i software maligni
5. prodotti con elementi digitali con funzione di rete privata virtuale (VPN)
6. sistemi di gestione della rete
7. sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM)
8. boot manager
9. infrastrutture a chiave pubblica e software per il rilascio di certificati digitali
10. interfacce di rete fisiche e virtuali
11. sistemi operativi
12. router, modem per la connessione a Internet e switch
13. microprocessori con funzionalità legate alla sicurezza
14. microcontrollori con funzionalità legate alla sicurezza
15. circuiti integrati per applicazioni specifiche (ASIC) e reti di porte programmabili dall'utilizzatore (FPGA) con funzionalità legate alla sicurezza
16. assistenti virtuali di uso generale per case intelligenti
17. prodotti per case intelligenti con funzionalità di sicurezza, tra cui serrature intelligenti, telecamere di sicurezza, sistemi di monitoraggio dei neonati e sistemi di allarme
18. giocattoli connessi a Internet disciplinati dalla direttiva 2009/48/CE del Parlamento europeo e del Consiglio [1] che presentano funzionalità sociali interattive (in grado ad esempio di parlare o filmare) o di geolocalizzazione
19. prodotti indossabili personali da indossare o collocare sul corpo umano a fini di monitoraggio della salute (come il tracciamento) e ai quali non si applica il regolamento (UE) 2017/745 o il regolamento (UE) 2017/746, o prodotti indossabili personali destinati all'uso da parte dei bambini e per questi ultimi

Classe II

1. ipervisori e sistemi di *runtime container* che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti simili
2. firewall, sistemi di rilevamento e prevenzione delle intrusioni
3. microprocessori a prova di manomissione
4. microcontrollori a prova di manomissione

---

[1] Direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli (GU L 170 del 30.6.2009, pag. 1).

ALLEGATO IV

PRODOTTI CON ELEMENTI DIGITALI CRITICI

1. Dispositivi hardware con cassette di sicurezza
2. gateway per contatori intelligenti nell'ambito di sistemi di misurazione intelligenti quali definiti all'articolo 2, punto 23), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio [1], e altri dispositivi a fini di sicurezza avanzati, compreso il trattamento crittografico sicuro
3. carte intelligenti o dispositivi analoghi, compresi gli elementi sicuri

[1] Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (GU L 158 del 14.6.2019, pag. 125).

ALLEGATO V

DICHIARAZIONE DI CONFORMITÀ UE

La dichiarazione di conformità UE di cui all'articolo 28 contiene tutte le informazioni seguenti:

1. nome e tipo e qualsiasi altra informazione che consenta l'identificazione univoca del prodotto con elementi digitali
2. nome e indirizzo del fabbricante o del suo rappresentante autorizzato
3. un'attestazione secondo cui la dichiarazione di conformità UE è rilasciata sotto la responsabilità esclusiva del fornitore
4. oggetto della dichiarazione (identificazione del prodotto con elementi digitali che ne consenta la tracciabilità, che può, se del caso, includere una fotografia)
5. un'attestazione secondo la quale l'oggetto della dichiarazione di cui sopra è conforme alla pertinente normativa di armonizzazione dell'Unione
6. riferimenti alle pertinenti norme armonizzate utilizzate o a qualsiasi altra specifica comune o certificazione di cibersicurezza in relazione alla quale è dichiarata la conformità
7. ove applicabile, il nome e il numero dell'organismo notificato, una descrizione della procedura di valutazione della conformità applicata e l'identificazione del certificato rilasciato
8. informazioni supplementari:

   Firmato a nome e per conto di:

   (luogo e data del rilascio):

   (nome, funzione) (firma):

ALLEGATO VI

DICHIARAZIONE DI CONFORMITÀ UE SEMPLIFICATA

La dichiarazione di conformità UE semplificata di cui all'articolo 13, paragrafo 20, deve essere presentata come segue:

Con la presente, … [nome del fabbricante] dichiara che il prodotto con elementi digitali … [denominazione del tipo di prodotto con elemento digitale] è conforme al regolamento (UE) 2024/2847 ([1]).

Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: …

([1]) GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

ALLEGATO VII

CONTENUTO DELLA DOCUMENTAZIONE TECNICA

La documentazione tecnica di cui all'articolo 31 include almeno le informazioni seguenti, a seconda dell'applicabilità al pertinente prodotto con elementi digitali:

1. una descrizione generale del prodotto con elementi digitali, tra cui:
   a) la finalità prevista;
   b) versioni del software importanti per la conformità ai requisiti essenziali di cibersicurezza;
   c) se il prodotto con elementi digitali consiste di un prodotto hardware, fotografie o illustrazioni che mostrino le caratteristiche esterne, la marcatura e la disposizione interna;
   d) informazioni e istruzioni per l'utilizzatore, come indicato nell'allegato II;
2. una descrizione della progettazione, dello sviluppo e della produzione del prodotto con elementi digitali e dei processi di gestione delle vulnerabilità, tra cui:
   a) le informazioni necessarie sulla progettazione e sullo sviluppo del prodotto con elementi digitali, compresi, se del caso, disegni e schemi e una descrizione dell'architettura del sistema che spieghi in che modo i componenti software si basano l'uno sull'altro o si alimentano reciprocamente e si integrano nel processo complessivo;
   b) le informazioni necessarie e specifiche sui processi di gestione delle vulnerabilità messi in atto dal fabbricante, tra cui la distinta base del software, la politica di gestione della divulgazione coordinata delle vulnerabilità, la prova della fornitura di un indirizzo di contatto per la segnalazione delle vulnerabilità e una descrizione delle soluzioni tecniche scelte per la distribuzione sicura degli aggiornamenti;
   c) le informazioni necessarie e specifiche relative ai processi di produzione e monitoraggio del prodotto con elementi digitali e alla convalida di tali processi;
3. una valutazione dei rischi di cibersicurezza a fronte dei quali il prodotto con elementi digitali è progettato, sviluppato, prodotto, consegnato e sottoposto a manutenzione, a norma dell'articolo 13, incluse le modalità di applicazione dei requisiti essenziali di cibersicurezza di cui all'allegato I, parte I;
4. informazioni pertinenti di cui si è tenuto conto per determinare il periodo di assistenza a norma dell'articolo 13, paragrafo 8, del prodotto con elementi digitali;
5. un elenco delle norme armonizzate applicate integralmente o in parte, i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, delle specifiche comuni di cui all'articolo 27 del presente regolamento o dei sistemi europei di certificazione della cibersicurezza adottati conformemente al regolamento (UE) 2019/881 a norma dell'articolo 27, paragrafo 8, del presente regolamento e, qualora non siano stati applicati tali norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza, le descrizioni delle soluzioni adottate per soddisfare i requisiti essenziali di cibersicurezza di cui all'allegato I, parti I e II, compreso un elenco delle altre pertinenti specifiche tecniche applicate. In caso di applicazione parziale delle norme armonizzate, delle specifiche comuni o dei sistemi europei di certificazione della cibersicurezza, la documentazione tecnica specifica le parti che sono state applicate;
6. le relazioni delle prove effettuate per verificare la conformità del prodotto con elementi digitali di cibersicurezza e dei processi di gestione delle vulnerabilità ai requisiti essenziali applicabili di cui all'allegato I, parti I e II;
7. una copia della dichiarazione di conformità UE;
8. se del caso, la distinta base del software, a seguito di una richiesta motivata di un'autorità di vigilanza del mercato, a condizione che ciò sia necessario affinché tale autorità possa verificare la conformità ai requisiti essenziali di cibersicurezza di cui all'allegato I.

ALLEGATO VIII

PROCEDURE DI VALUTAZIONE DELLA CONFORMITÀ

Parte I Procedura di valutazione della conformità basata sul controllo interno (basata sul modulo A)

1. Il controllo interno è la procedura di valutazione della conformità con cui il fabbricante adempie agli obblighi stabiliti ai punti 2, 3 e 4 della presente parte e garantisce e dichiara, sotto la sua esclusiva responsabilità, che i prodotti con elementi digitali soddisfano tutti i requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e che il fabbricante soddisfa i requisiti essenziali di cibersicurezza di cui all'allegato I, parte II.

2. Il fabbricante redige la documentazione tecnica di cui all'allegato VII.

3. Progettazione, sviluppo, produzione e gestione delle vulnerabilità dei prodotti con elementi digitali

   Il fabbricante adotta tutte le misure necessarie affinché i processi di progettazione, sviluppo, produzione e gestione delle vulnerabilità e il loro monitoraggio garantiscano la conformità dei prodotti con elementi digitali fabbricati o sviluppati e dei processi messi in atto dal fabbricante ai requisiti essenziali di cibersicurezza di cui all'allegato I, parti I e II.

4. Marcatura di conformità e dichiarazione di conformità

   4.1. Il fabbricante appone la marcatura CE ad ogni singolo prodotto con elementi digitali che soddisfa i requisiti applicabili stabiliti nel presente regolamento.

   4.2. Per ciascun prodotto con elementi digitali il fabbricante compila una dichiarazione di conformità UE scritta in conformità dell'articolo 28 che, insieme alla documentazione tecnica, lascia a disposizione delle autorità nazionali per dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per il periodo di assistenza, se quest'ultimo è superiore. La dichiarazione di conformità UE identifica il prodotto con elementi digitali per cui è stata compilata. Una copia della dichiarazione di conformità UE è messa a disposizione delle autorità competenti su richiesta.

5. Rappresentanti autorizzati

   Gli obblighi del fabbricante previsti al punto 4 possono essere adempiuti dal suo rappresentante autorizzato, a nome del fabbricante e sotto la sua responsabilità, purché gli obblighi pertinenti siano specificati nel mandato.

Parte II Esame UE del tipo (basato sul modulo B)

1. L'esame UE del tipo è la parte di una procedura di valutazione della conformità in cui un organismo notificato esamina la progettazione tecnica e lo sviluppo di un prodotto con elementi digitali e i processi di gestione delle vulnerabilità messi in atto dal fabbricante e attesta che un prodotto con elementi digitali soddisfa i requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e che il fabbricante soddisfa i requisiti essenziali di cibersicurezza di cui all'allegato I, parte II.

2. L'esame UE del tipo è realizzato in base a una valutazione dell'adeguatezza della progettazione tecnica e dello sviluppo del prodotto con elementi digitali, effettuata esaminando la documentazione tecnica e di supporto di cui al punto 3 ed esaminando i campioni di una o più parti critiche del prodotto (combinazione tra tipo di produzione e tipo di progetto).

3. Il fabbricante presenta una domanda di esame UE del tipo a un unico organismo notificato di sua scelta.

   La domanda contiene:

   3.1. il nome e l'indirizzo del fabbricante e, qualora la domanda sia presentata dal suo rappresentante autorizzato, il nome e l'indirizzo di quest'ultimo;

   3.2. una dichiarazione scritta in cui si precisa che la stessa domanda non è stata presentata a nessun altro organismo notificato;

   3.3. la documentazione tecnica, che consente di valutare la conformità del prodotto con elementi digitali ai requisiti essenziali di cibersicurezza applicabili di cui all'allegato I, parte I, e dei processi di gestione delle vulnerabilità messi in atto dal fabbricante ai requisiti di cui all'allegato I, parte II, e che include un'analisi e una valutazione adeguate dei rischi. Essa precisa i requisiti applicabili e comprende, nella misura necessaria ai fini della valutazione, il progetto, la fabbricazione e il funzionamento del prodotto con elementi digitali. La documentazione tecnica contiene, laddove applicabile, almeno gli elementi di cui all'allegato VII;

3.4. la documentazione di supporto attestante l'adeguatezza delle soluzioni di progettazione tecnica e sviluppo e dei processi di gestione delle vulnerabilità. Tale documentazione di supporto elenca tutti i documenti che sono stati utilizzati, soprattutto nel caso in cui le norme armonizzate o le specifiche tecniche pertinenti non siano state applicate integralmente. La documentazione di supporto comprende, ove necessario, i risultati delle prove effettuate dall'apposito laboratorio del fabbricante o da un altro laboratorio di prova, per conto e sotto la responsabilità del fabbricante.

4. L'organismo notificato:

4.1. esamina la documentazione tecnica e di supporto per valutare l'adeguatezza della progettazione tecnica e dello sviluppo del prodotto con elementi digitali ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e dei processi di gestione delle vulnerabilità messi in atto dal fabbricante ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte II;

4.2. verifica che i campioni siano stati sviluppati o fabbricati in conformità della documentazione tecnica e individua gli elementi progettati e sviluppati in conformità delle disposizioni applicabili delle norme armonizzate o delle specifiche tecniche pertinenti, nonché gli elementi progettati e sviluppati senza applicare le disposizioni pertinenti previste da tali norme;

4.3. effettua o fa effettuare esami e prove appropriati per controllare che, qualora il fabbricante abbia scelto di applicare le soluzioni di cui alle norme armonizzate o alle specifiche tecniche pertinenti per i requisiti di cui all'allegato I, tali soluzioni siano state applicate correttamente;

4.4. effettua o fa effettuare esami e prove appropriati per controllare che, laddove non siano state applicate le soluzioni di cui alle norme armonizzate o alle specifiche tecniche pertinenti per i requisiti di cui all'allegato I, le soluzioni adottate dal fabbricante soddisfino i requisiti essenziali di cibersicurezza corrispondenti;

4.5. concorda con il fabbricante il luogo in cui dovranno essere effettuati gli esami e le prove.

5. L'organismo notificato redige una relazione di valutazione che elenca le iniziative intraprese in conformità del punto 4 e i relativi risultati. Senza pregiudicare i propri obblighi di fronte alle autorità di notifica, l'organismo notificato rende pubblico l'intero contenuto della relazione, o parte di esso, solo con l'accordo del fabbricante.

6. Se il tipo e i processi di gestione delle vulnerabilità soddisfano i requisiti essenziali di cibersicurezza di cui all'allegato I, l'organismo notificato rilascia al fabbricante un certificato di esame UE del tipo. Il certificato indica nome e indirizzo del fabbricante, le conclusioni dell'esame, le eventuali condizioni di validità e i dati necessari per identificare il tipo omologato e i processi di gestione delle vulnerabilità. Il certificato può avere uno o più allegati.

Il certificato e i suoi allegati contengono tutte le informazioni pertinenti per consentire la valutazione della conformità dei prodotti con elementi digitali fabbricati o sviluppati al tipo esaminato e dei processi di gestione delle vulnerabilità e permettere il controllo dei prodotti in funzione.

Se il tipo e i processi di gestione delle vulnerabilità non soddisfano i requisiti essenziali di cibersicurezza applicabili di cui all'allegato I, l'organismo notificato rifiuta di rilasciare un certificato di esame UE del tipo e informa di tale decisione il richiedente, motivando dettagliatamente il suo rifiuto.

7. L'organismo notificato segue l'evoluzione del progresso tecnologico generalmente riconosciuto, in base al quale il tipo omologato e i processi di gestione delle vulnerabilità potrebbero non essere più conformi ai requisiti essenziali di cibersicurezza applicabili di cui all'allegato I, e decide se tale progresso richieda ulteriori indagini. In caso affermativo, l'organismo notificato ne informa il fabbricante.

Il fabbricante informa l'organismo notificato che detiene la documentazione tecnica relativa al certificato di esame UE del tipo di tutte le modifiche al tipo omologato e ai processi di gestione delle vulnerabilità che possono influire sulla conformità ai requisiti essenziali di cibersicurezza di cui all'allegato I o sulle condizioni di validità del certificato. Tali modifiche comportano una nuova approvazione, sotto forma di un supplemento al certificato originario di esame UE del tipo.

8. L'organismo notificato svolge audit periodici per garantire che i processi di gestione delle vulnerabilità di cui all'allegato I, parte II, siano attuati adeguatamente.

9. Ogni organismo notificato informa le proprie autorità di notifica dei certificati di esame UE del tipo o dei relativi supplementi da esso rilasciati o ritirati e mette a disposizione di tali autorità, periodicamente o su richiesta, l'elenco dei certificati o dei relativi supplementi respinti, sospesi o altrimenti sottoposti a restrizioni.

   Ogni organismo notificato informa gli altri organismi notificati in merito ai certificati di esame UE del tipo o agli eventuali supplementi da esso rifiutati, ritirati, sospesi o altrimenti sottoposti a restrizioni e, su richiesta, in merito ai certificati o agli eventuali supplementi da esso rilasciati.

   La Commissione, gli Stati membri e gli altri organismi notificati possono ottenere, su richiesta, copia dei certificati di esame UE del tipo e di qualsiasi loro supplemento. La Commissione e gli Stati membri possono ottenere, su richiesta, copia della documentazione tecnica e dei risultati degli esami effettuati dall'organismo notificato. L'organismo notificato conserva una copia del certificato di esame UE del tipo e dei relativi allegati e supplementi, nonché il fascicolo tecnico contenente la documentazione presentata dal fabbricante, fino alla scadenza della validità del certificato.

10. Il fabbricante tiene a disposizione delle autorità nazionali una copia del certificato di esame UE del tipo e dei relativi allegati e supplementi insieme alla documentazione tecnica per dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per il periodo di assistenza, se quest'ultimo è superiore.

11. Il rappresentante autorizzato del fabbricante può presentare la domanda di cui al punto 3 e ottemperare agli obblighi di cui ai punti 7 e 10, purché gli obblighi pertinenti siano specificati nel mandato.

Parte III Conformità al tipo basata sul controllo interno della produzione (basata sul modulo C)

1. La conformità al tipo basata sul controllo interno della produzione è la parte di una procedura di valutazione della conformità con cui il fabbricante ottempera agli obblighi stabiliti ai punti 2 e 3 della presente parte e si accerta e dichiara che i prodotti con elementi digitali interessati sono conformi al tipo descritto nel certificato di esame UE del tipo e soddisfano i requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e che il fabbricante soddisfa i requisiti essenziali di cibersicurezza di cui all'allegato I, parte II.

2. Produzione

   Il fabbricante adotta tutte le misure necessarie affinché il processo di produzione e il suo controllo garantiscano la conformità dei prodotti con elementi digitali fabbricati al tipo omologato descritto nel certificato di esame UE del tipo e ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e si accerta che il fabbricante soddisfa i requisiti essenziali di cibersicurezza di cui all'allegato I, parte II.

3. Marcatura di conformità e dichiarazione di conformità

   3.1. Il fabbricante appone la marcatura CE a ogni singolo prodotto con elementi digitali conforme al tipo descritto nel certificato di esame UE del tipo e ai requisiti applicabili stabiliti nel presente regolamento.

   3.2. Il fabbricante compila una dichiarazione scritta di conformità per un modello di prodotto e la tiene a disposizione delle autorità nazionali per dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per il periodo di assistenza, se quest'ultimo è superiore. La dichiarazione di conformità identifica il modello di prodotto per cui è stata compilata. Una copia di tale dichiarazione è messa a disposizione delle autorità competenti su richiesta.

4. Rappresentante autorizzato

   Gli obblighi del fabbricante di cui al punto 3 possono essere adempiuti dal suo rappresentante autorizzato, a nome del fabbricante e sotto la sua responsabilità, purché gli obblighi pertinenti siano specificati nel mandato.

Parte IV Conformità basata sulla garanzia della qualità totale (basata sul modulo H)

1. La conformità basata sulla garanzia della qualità totale è la procedura di valutazione della conformità con cui il fabbricante ottempera agli obblighi stabiliti ai punti 2 e 5 della presente parte e garantisce e dichiara, sotto la sua esclusiva responsabilità, che i prodotti con elementi digitali o le categorie di prodotti interessati soddisfano i requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e che i processi di gestione delle vulnerabilità messi in atto dal fabbricante soddisfano i requisiti di cui all'allegato I, parte II.

2. Progettazione, sviluppo, produzione e gestione delle vulnerabilità dei prodotti con elementi digitali

Il fabbricante applica un sistema qualità approvato, come specificato al punto 3, per la progettazione, lo sviluppo nonché l'ispezione e la prova finali dei prodotti con elementi digitali interessati e per la gestione delle vulnerabilità, ne mantiene l'efficacia nel corso di tutto il periodo di assistenza ed è assoggettato alla sorveglianza di cui al punto 4.

3. Sistema qualità

3.1. Il fabbricante presenta una domanda per la valutazione del suo sistema qualità per i prodotti con elementi digitali interessati all'organismo notificato di sua scelta.

La domanda contiene:

a) il nome e l'indirizzo del fabbricante e, qualora la domanda sia presentata dal suo rappresentante autorizzato, il nome e l'indirizzo di quest'ultimo;

b) la documentazione tecnica per un modello di ciascuna categoria di prodotti con elementi digitali che intende fabbricare o sviluppare. La documentazione tecnica contiene, laddove applicabile, almeno gli elementi di cui all'allegato VII;

c) la documentazione relativa al sistema qualità; nonché

d) una dichiarazione scritta in cui si precisa che la stessa domanda non è stata presentata a nessun altro organismo notificato.

3.2. Il sistema qualità garantisce la conformità dei prodotti con elementi digitali ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, e la conformità dei processi di gestione delle vulnerabilità messi in atto dal fabbricante ai requisiti di cui all'allegato I, parte II.

Tutti i criteri, i requisiti e le disposizioni adottati dal fabbricante sono documentati in modo sistematico e ordinato sotto forma di misure, procedure e istruzioni scritte. Tale documentazione relativa al sistema qualità consente un'interpretazione uniforme di programmi, schemi, manuali e registri riguardanti la qualità.

Essa include in particolare un'adeguata descrizione:

a) degli obiettivi di qualità e della struttura organizzativa, delle responsabilità e dei poteri del personale direttivo in materia di progettazione, sviluppo, qualità del prodotto e gestione delle vulnerabilità;

b) delle specifiche di progettazione tecnica e di sviluppo, comprese le norme, che saranno applicate e, qualora non siano applicate integralmente le norme armonizzate o le specifiche tecniche pertinenti, degli strumenti che saranno utilizzati per garantire l'osservanza dei requisiti essenziali di cibersicurezza di cui all'allegato I, parte I, che si applicano ai prodotti con elementi digitali;

c) delle specifiche procedurali, comprese le norme, che saranno applicate e, qualora non siano applicate integralmente le norme armonizzate e le specifiche tecniche pertinenti, degli strumenti che saranno utilizzati per garantire l'osservanza dei requisiti essenziali di cibersicurezza di cui all'allegato I, parte II, che si applicano al fabbricante;

d) delle tecniche, dei processi e degli interventi sistematici in materia di controllo e verifica della progettazione e dello sviluppo che saranno applicati nella progettazione e nello sviluppo dei prodotti con elementi digitali appartenenti alla categoria di prodotti in questione;

e) delle tecniche, dei processi e degli interventi sistematici che saranno applicati nella produzione, nel controllo di qualità e nella garanzia della qualità;

f) degli esami e delle prove che saranno effettuati prima, durante e dopo la produzione, con indicazione della frequenza con cui si intende effettuarli;

g) della documentazione in materia di qualità, quali le relazioni sulle ispezioni, i dati relativi alle prove e alle tarature e i rapporti sulle qualifiche del personale interessato;

h) dei mezzi di controllo delle modalità per ottenere la qualità di progettazione e la qualità del prodotto richieste e dell'efficace funzionamento del sistema qualità.

3.3. L'organismo notificato valuta il sistema qualità per determinare se soddisfa i requisiti di cui al punto 3.2.

L'organismo presume la conformità a tali requisiti degli elementi del sistema qualità conformi alle specifiche corrispondenti della norma nazionale che attua la norma armonizzata o la specifica tecnica pertinente.

Oltre ad avere esperienza nei sistemi di gestione della qualità, almeno un membro del gruppo incaricato dell'audit ha esperienza nella valutazione del settore e della tecnologia del prodotto in questione e conosce i requisiti applicabili stabiliti nel presente regolamento. L'audit prevede una visita di valutazione dei locali del fabbricante, ove esistenti. Il gruppo incaricato dell'audit esamina la documentazione tecnica di cui al punto 3.1, lettera b), per verificare la capacità del fabbricante di individuare i requisiti applicabili stabiliti nel presente regolamento e di effettuare gli esami necessari atti a garantire la conformità del prodotto con elementi digitali a tali requisiti.

La decisione è notificata al fabbricante o al suo rappresentante autorizzato.

La notifica contiene le conclusioni dell'audit e la motivazione circostanziata della decisione.

3.4. Il fabbricante si impegna a soddisfare gli obblighi derivanti dal sistema qualità approvato e a fare in modo che esso rimanga adeguato ed efficace.

3.5. Il fabbricante tiene informato l'organismo notificato che ha approvato il sistema qualità delle modifiche che intende apportare a tale sistema.

L'organismo notificato valuta le modifiche proposte e decide se il sistema qualità modificato continui a soddisfare i requisiti di cui al punto 3.2 o se sia necessaria una nuova verifica.

Esso notifica la decisione al fabbricante. La notifica contiene le conclusioni dell'esame e la motivazione circostanziata della decisione.

4. Sorveglianza sotto la responsabilità dell'organismo notificato

4.1. Scopo della sorveglianza è garantire che il fabbricante ottemperi debitamente agli obblighi derivanti dal sistema qualità approvato.

4.2. Il fabbricante consente all'organismo notificato di accedere, ai fini della valutazione, ai locali di progettazione, sviluppo, produzione, ispezione, prova e deposito fornendo tutte le necessarie informazioni, in particolare:

a) la documentazione relativa al sistema qualità;

b) la documentazione in materia di qualità prevista nella sezione del sistema qualità riservata alla progettazione, come i risultati di analisi, calcoli e prove;

c) la documentazione in materia di qualità prevista nella sezione del sistema qualità relativa alla fabbricazione, come le relazioni sulle ispezioni, i dati relativi alle prove e alle tarature e i rapporti sulle qualifiche del personale interessato.

4.3. L'organismo notificato svolge audit periodici intesi ad accertare che il fabbricante mantenga e applichi il sistema qualità e fornisce al fabbricante una relazione sugli audit effettuati.

5. Marcatura di conformità e dichiarazione di conformità

5.1. Il fabbricante appone la marcatura CE e, sotto la responsabilità dell'organismo notificato di cui al punto 3.1, il numero di identificazione di quest'ultimo, su ogni singolo prodotto con elementi digitali che soddisfa i requisiti di cui all'allegato I, parte I.

5.2. Il fabbricante compila una dichiarazione di conformità per ciascun modello di prodotto e la tiene a disposizione delle autorità nazionali per un periodo di dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per il periodo di assistenza, se quest'ultimo è superiore. La dichiarazione di conformità identifica il modello di prodotto per cui è stata compilata.

Una copia di tale dichiarazione è messa a disposizione delle autorità competenti su richiesta.

6. Il fabbricante, per almeno dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per il periodo di assistenza, se quest'ultimo è superiore, tiene a disposizione delle autorità nazionali:

a) la documentazione tecnica di cui al punto 3.1;

b) la documentazione relativa al sistema qualità di cui al punto 3.1;

c) le modifiche di cui al punto 3.5 e la relativa approvazione;

d) le decisioni e le relazioni trasmesse dall'organismo notificato di cui ai punti 3.5 e 4.3.

7. Ogni organismo notificato informa le proprie autorità di notifica delle approvazioni dei sistemi qualità rilasciate o ritirate e, periodicamente o su richiesta, mette a loro disposizione l'elenco delle approvazioni dei sistemi qualità respinte, sospese o altrimenti sottoposte a restrizioni.

Ogni organismo notificato informa gli altri organismi notificati delle approvazioni dei sistemi qualità da esso rifiutate, sospese o ritirate e, a richiesta, delle approvazioni dei sistemi qualità rilasciate.

8. Rappresentante autorizzato

Gli obblighi del fabbricante di cui ai punti 3.1, 3.5, 5 e 6 possono essere adempiuti dal suo rappresentante autorizzato, a nome del fabbricante e sotto la sua responsabilità, purché gli obblighi pertinenti siano specificati nel mandato.

In relazione al presente atto è stata formulata una dichiarazione che figura nella GU C, 2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj.