

2. Qualora abbia motivo sufficiente di ritenere che un sistema di IA ad alto rischio non sia conforme al presente regolamento, ovvero sia falsificato o sia accompagnato da una documentazione falsificata, un importatore non lo immette sul mercato fino a quando non sia stato reso conforme. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, l'importatore ne informa il fornitore del sistema, i rappresentanti autorizzati e le autorità di vigilanza del mercato.
3. Gli importatori indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato e l'indirizzo al quale possono essere contattati, sul sistema di IA ad alto rischio e sul suo imballaggio o in un documento di accompagnamento, ove applicabile.
4. Gli importatori garantiscono che, fintantoché un sistema di IA ad alto rischio è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto, ove applicabili, non pregiudichino la conformità ai requisiti di cui alla sezione 2.
5. Gli importatori conservano, per un periodo di 10 anni dalla data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, una copia del certificato rilasciato dall'organismo notificato, se del caso, delle istruzioni per l'uso e della dichiarazione di conformità UE di cui all'articolo 47.
6. Gli importatori forniscono alla pertinente autorità competente, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle di cui al paragrafo 5, necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2 in una lingua che può essere compresa facilmente da tale autorità nazionale competente. A tal fine garantiscono altresì che la documentazione tecnica possa essere messa a disposizione di tale autorità.
7. Gli importatori cooperano con le pertinenti autorità competenti in qualsiasi azione intrapresa da tali autorità in relazione a un sistema di IA ad alto rischio immesso sul mercato dagli importatori, in particolare per ridurre e attenuare i rischi che esso comporta.

Articolo 24

Obblighi dei distributori

1. Prima di mettere a disposizione sul mercato un sistema di IA ad alto rischio, i distributori verificano che esso rechi la necessaria marcatura CE, che sia accompagnato da una copia della dichiarazione di conformità UE di cui all'articolo 47 e dalle istruzioni per l'uso e che il fornitore e l'importatore di tale sistema, a seconda dei casi, abbiano rispettato i loro rispettivi obblighi di cui all'articolo 16, lettere b) e c), e all'articolo 23, paragrafo 3.
2. Qualora ritenga o abbia motivo di ritenere, sulla base delle informazioni in suo possesso, che un sistema di IA ad alto rischio non sia conforme ai requisiti di cui alla sezione 2, un distributore non lo mette a disposizione sul mercato fino a quando tale sistema di IA ad alto rischio non sia stato reso conforme a tali requisiti. Inoltre, qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, il distributore ne informa il fornitore o l'importatore del sistema, a seconda dei casi.
3. I distributori garantiscono che, fintantoché un sistema di IA ad alto rischio è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto, ove applicabili, non pregiudichino la conformità del sistema ai requisiti di cui alla sezione 2.
4. Un distributore che ritiene o ha motivo di ritenere, sulla base delle informazioni in suo possesso, che un sistema di IA ad alto rischio che ha messo a disposizione sul mercato non sia conforme ai requisiti di cui alla sezione 2, adotta le misure correttive necessarie per rendere tale sistema conforme a tali requisiti, ritirarlo o richiamarlo o garantisce che il fornitore, l'importatore o qualsiasi operatore pertinente, a seconda dei casi, adotti tali misure correttive. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, il distributore ne informa immediatamente il fornitore o l'importatore del sistema e le autorità competenti per il sistema di IA ad alto rischio interessate fornendo in particolare informazioni precise sulla non conformità e sulle eventuali misure correttive adottate.
5. Su richiesta motivata di una pertinente autorità competente, i distributori di un sistema di IA ad alto rischio forniscono a tale autorità tutte le informazioni e la documentazione concernenti le sue azioni a norma dei paragrafi da 1 a 4 necessarie per dimostrare la conformità di tale sistema ai requisiti di cui alla sezione 2.
6. I distributori cooperano con le pertinenti autorità competenti in qualsiasi azione intrapresa da tali autorità in relazione a un sistema di IA ad alto rischio messo a disposizione sul mercato dai distributori, in particolare per ridurre e attenuare il rischio che esso comporta.

*Articolo 25***Responsabilità lungo la catena del valore dell'IA**

1. Qualsiasi distributore, importatore, deployer o altro terzo è considerato fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore a norma dell'articolo 16, nelle circostanze seguenti:

- a) se appone il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi al riguardo;
- b) se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o già messo in servizio in modo tale che resti un sistema di IA ad alto rischio a norma dell'articolo 6;
- c) se modifica la finalità prevista di un sistema di IA, anche un sistema per finalità generali, che non è stato classificato come ad alto rischio e che è già stato immesso sul mercato o messo in servizio in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6.

2. Qualora si verifichino le circostanze di cui al paragrafo 1, il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA non è più considerato fornitore di quel determinato sistema di IA ai fini del presente regolamento. Tale fornitore iniziale coopera strettamente con i nuovi fornitori e mette a disposizione le informazioni necessarie nonché fornisce l'accesso tecnico ragionevolmente atteso e qualsiasi altra forma di assistenza che sono richiesti per l'adempimento degli obblighi di cui al presente regolamento, in particolare per quanto riguarda la conformità alla valutazione della conformità dei sistemi di IA ad alto rischio. Il presente paragrafo non si applica nei casi in cui il fornitore iniziale abbia chiaramente specificato che il suo sistema di IA non deve essere trasformato in un sistema di IA ad alto rischio e pertanto non sia soggetto all'obbligo di consegnare la documentazione.

3. Nel caso dei sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, il fabbricante del prodotto è considerato il fornitore del sistema di IA ad alto rischio ed è soggetto agli obblighi di cui all'articolo 16, in una delle circostanze seguenti:

- a) se il sistema di IA ad alto rischio è immesso sul mercato insieme al prodotto con il nome o il marchio del fabbricante del prodotto;
- b) se il sistema di IA ad alto rischio è messo in servizio con il nome o il marchio del fabbricante del prodotto dopo che il prodotto è stato immesso sul mercato.

4. Il fornitore di un sistema di IA ad alto rischio e il terzo che fornisce un sistema di IA, strumenti, servizi, componenti o processi utilizzati o integrati in un sistema di IA ad alto rischio precisano, mediante accordo scritto, le informazioni, le capacità, l'accesso tecnico e qualsiasi altra forma di assistenza necessari, sulla base dello stato dell'arte generalmente riconosciuto per permettere al fornitore del sistema di IA ad alto rischio di adempiere pienamente agli obblighi di cui al presente regolamento. Il presente paragrafo non si applica ai terzi che rendono accessibili al pubblico strumenti, servizi, processi o componenti, diversi dai modelli di IA per finalità generali, con licenza libera e open source.

L'ufficio per l'IA può elaborare e raccomandare clausole contrattuali tipo volontarie tra i fornitori di sistemi di IA ad alto rischio e i terzi che forniscono strumenti, servizi, componenti o processi utilizzati o integrati in sistemi di IA ad alto rischio. Nell'elaborare tali clausole contrattuali tipo volontarie, l'ufficio per l'IA tiene conto dei possibili requisiti contrattuali applicabili in determinati settori o casi commerciali. Le clausole contrattuali tipo volontarie sono pubblicati e disponibili gratuitamente in un formato elettronico facilmente utilizzabile.

5. I paragrafi 2 e 3 lasciano impregiudicata la necessità di rispettare e proteggere i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti commerciali conformemente al diritto dell'Unione e nazionale.

*Articolo 26***Obblighi dei deployer dei sistemi di IA ad alto rischio**

1. I deployer di sistemi di IA ad alto rischio adottano idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 3 e 6.

2. I deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario.

3. Gli obblighi di cui ai paragrafi 1 e 2 lasciano impregiudicati gli altri obblighi dei deployer previsti dal diritto dell'Unione o nazionale e la libertà del deployer di organizzare le proprie risorse e attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore.

4. Fatti salvi i paragrafi 1 e 2, nella misura in cui esercita il controllo sui dati di input, il deployer garantisce che tali dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista del sistema di IA ad alto rischio.

5. I deployer monitorano il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informano i fornitori a tale riguardo conformemente all'articolo 72. Qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa comportare che il sistema di IA presenti un rischio ai sensi dell'articolo 79, paragrafo 1, i deployer ne informano, senza indebito ritardo, il fornitore o il distributore e la pertinente autorità di vigilanza del mercato e sospendono l'uso di tale sistema. Qualora abbiano individuato un incidente grave, i deployer ne informano immediatamente anche il fornitore, in primo luogo, e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato. Nel caso in cui il deployer non sia in grado di raggiungere il fornitore, si applica mutatis mutandis l'articolo 73. Tale obbligo non riguarda i dati operativi sensibili dei deployer dei sistemi di IA che sono autorità di contrasto.

Per i deployer che sono istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di monitoraggio di cui al primo comma si considera soddisfatto se sono soddisfatte le regole sui dispositivi, sui processi e sui meccanismi di governance interna a norma del pertinente diritto in materia di servizi finanziari.

6. I deployer di sistemi di IA ad alto rischio conservano i log generati automaticamente da tale sistema di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo, per un periodo adeguato alla prevista finalità del sistema di IA ad alto rischio, di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali.

I deployer che sono istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari conservano i log come parte della documentazione conservata a norma del pertinente diritto dell'Unione in materia di servizi finanziari.

7. Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti.

8. I deployer di sistemi di IA ad alto rischio che sono autorità pubbliche o istituzioni, organi e organismi dell'Unione rispettano gli obblighi di registrazione di cui all'articolo 49. Ove accertino che il sistema di IA ad alto rischio che intendono utilizzare non è stato registrato nella banca dati dell'UE di cui all'articolo 71, tali deployer non utilizzano tale sistema e ne informano il fornitore o il distributore.

9. Se del caso, i deployer di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 del presente regolamento per adempiere al loro obbligo di effettuare una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680.

10. Fatta salva la direttiva (UE) 2016/680, nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato, il deployer di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori chiede un'autorizzazione, *ex ante* o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato. Ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato.

Se l'autorizzazione richiesta a norma del primo comma è respinta, l'uso del sistema di identificazione biometrica remota a posteriori collegato a tale autorizzazione richiesta è interrotto con effetto immediato e i dati personali connessi all'uso del sistema di IA ad alto rischio per il quale è stata richiesta l'autorizzazione sono cancellati.