5 Commentario all'Accordo multilaterale delle Autorità competenti

Introduzione

1. Per poter scambiare informazioni in virtù del Quadro per la comunicazione di informazioni in materia di cripto-attività (CARF), le giurisdizioni devono disporre di un quadro giuridico che consenta lo scambio automatico di informazioni con le giurisdizioni partner. Tale quadro giuridico dovrebbe includere sia una base legale giuridica per lo scambio di informazioni, sia accordi amministrativi per determinare l'ambito di applicazione, le tempistiche e le modalità dello scambio di informazioni.

2. Le giurisdizioni possono disporre di una base giuridica per lo scambio di informazioni fiscali in virtù della Convenzione sulla mutua assistenza amministrativa in materia fiscale (la "Convenzione"). Ai sensi dell'articolo 6 della Convenzione, due o più Parti della Convenzione possono concordare di scambiare automaticamente informazioni prevedibilmente pertinenti predefinite, secondo le procedure stabilite dalle Parti di comune accordo. Nel contesto dello Standard comune di comunicazione di informazioni, questo approccio multilaterale si è rivelato un mezzo efficace per la creazione di reti diffuse di rapporti di scambio, poiché consente alle giurisdizioni di attivare in modo efficiente rapporti di scambio bilaterali.

3. Per rendere operativo l'articolo 6 della Convenzione, le giurisdizioni devono anche disporre di accordi amministrativi per determinare, in particolare, le informazioni da scambiare automaticamente nonché le tempistiche e le modalità degli scambi. Per il CARF, questo Accordo multilaterale tra Autorità competenti per lo scambio automatico di informazioni (CARF MCAA), che si basa sull'articolo 6 della Convenzione, definisce le modalità dettagliate degli scambi che avvengono ogni anno su base automatica.

4. Il CARF MCAA è composto da:

- una dichiarazione che l'Autorità competente della giurisdizione o il suo rappresentante designato devono firmare per diventare firmatari del CARF MCAA;
- un preambolo che spiega le finalità del CARF MCAA e contiene le dichiarazioni relative alle norme nazionali in materia di obblighi di comunicazione e di adeguata verifica in materia fiscale che costituiscono la base dello scambio di informazioni basato sul CARF MCAA. Esso contiene inoltre le dichiarazioni relative alla riservatezza, alle garanzie per la protezione dei dati e sull'esistenza dell'infrastruttura necessaria;
- otto sezioni contenenti le disposizioni concordate del CARF MCAA: la sezione 1 riguarda le definizioni, la sezione 2 gli elementi delle informazioni oggetto di scambio, la sezione 3 i tempi e le modalità dello scambio, la sezione 4 la collaborazione in materia di conformità e applicazione e la sezione 5 gli obblighi in materia di riservatezza e protezione dei dati da rispettare. Le consultazioni tra le Autorità competenti, le modifiche al CARF MCAA e i termini generali del CARF MCAA, compresa l'attivazione dei rapporti di scambio attraverso la

presentazione di notifiche, la sospensione, la disattivazione e la cessazione, nonché il ruolo del Segretariato dell'organo di coordinamento, sono trattati nelle sezioni 6, 7 e 8;

- sette notifiche previste ai sensi della sezione 7, punto 1), ai fini dell'entrata in vigore del CARF MCAA nei confronti di un'Autorità competente.

5. Il CARF MCAA è un accordo multilaterale basato sul principio della reciprocità e bilateralità dello scambio automatico. Alcuni casi prevedono che le Autorità competenti possano instaurare un rapporto di scambio bilaterale non reciproco (ad esempio, nel caso in cui una giurisdizione non preveda un'imposta sul reddito), che deve essere confermato in una notifica fornita ai sensi della sezione 7, punto 1), lettera b).

6. In alternativa al CARF MCAA, le giurisdizioni possono anche stabilire relazioni di scambio automatico attraverso accordi bilaterali con le Autorità competenti basati su trattati bilaterali contro la doppia imposizione o su accordi sullo scambio di informazioni ai fini fiscali che consentono lo scambio automatico di informazioni, o sulla Convenzione sulla mutua assistenza amministrativa in materia fiscale. Le giurisdizioni possono anche stipulare un accordo intergovernativo autonomo o fare riferimento a una legislazione regionale che disciplini sia gli obblighi di comunicazione sia le procedure di adeguata verifica in materia fiscale in combinazione con le modalità di scambio di informazioni.

Commentario alla dichiarazione

1. Per diventare firmataria del CARF MCAA, l'Autorità competente della giurisdizione, o il suo rappresentante designato, deve firmare la dichiarazione e trasmetterla, insieme al testo del CARF MCAA, al Segretariato dell'organo di coordinamento.

2. Il CARF MCAA entrerà in vigore nei confronti di un'altra Autorità competente solo quando entrambe le Autorità competenti avranno firmato la dichiarazione, avranno presentato tutte le notifiche correlate ai sensi della sezione 7, punto 1) al Segretariato dell'organo di coordinamento e si saranno iscritte reciprocamente nell'elenco dei partner di scambio previsti nella notifica fornita conformemente alla sezione 7, punto 1), lettera g).

Commentario al preambolo

1. Il preambolo ("i considerando") definisce il contesto, illustra lo scopo del CARF MCAA e contiene le dichiarazioni dei firmatari.

2. Il primo considerando conferma che le giurisdizioni dei firmatari del CARF MCAA sono Parti o territori contemplati dalla Convenzione, condizione necessaria per poter firmare l'accordo.

3. Il secondo e il terzo considerando fungono da introduzione e chiariscono che lo scopo del CARF MCAA consiste nel contrastare l'elusione e l'evasione fiscale nonché di migliorare l'adempimento fiscale.

4. Il quarto considerando stabilisce che le Autorità competenti dichiarino che le leggi delle rispettive giurisdizioni impongano, o si prevede che impongano, ai prestatori di servizi per le cripto-attività con obbligo di comunicazione di comunicare informazioni relative alle cripto-attività pertinenti, coerentemente con l'ambito di scambio contemplato dalla sezione 2. La formulazione utilizzata nel quarto considerando consente alle Autorità competenti che lo desiderino di firmare il CARF MCAA prima che la loro giurisdizione disponga delle norme pertinenti di adeguata verifica in materia fiscale e di comunicazione.

5. Il quinto considerando prevede che le future modifiche al Quadro per la comunicazione di informazioni in materia di cripto-attività siano recepite nella legislazione nazionale delle giurisdizioni e che, una volta promulgate da una giurisdizione, qualsiasi riferimento al termine "quadro per la comunicazione

di informazioni in materia di cripto-attività" sia inteso come facente riferimento alla versione modificata in relazione a tale giurisdizione.

6. Il sesto considerando sancisce la base giuridica che autorizza lo scambio automatico di informazioni e consente alle Autorità competenti di concordare le procedure da applicare a tali scambi automatici. L'ambito di applicazione concordato è conforme all'ambito di scambio contemplato dalla sezione 2.

7. Il settimo considerando specifica che, laddove la Convenzione consenta a due o più Parti di concordare reciprocamente lo scambio automatico di informazioni specifiche, l'effettivo scambio di informazioni avverrà su base bilaterale (ovvero dall'Autorità competente mittente all'Autorità competente destinataria).

8. L'ottavo considerando stabilisce che le Autorità competenti dichiarino che le loro giurisdizioni dispongono di i) adeguate salvaguardie per assicurare la riservatezza delle informazioni ricevute e ii) un'infrastruttura che consente un rapporto di scambio efficace.

9. Il nono considerando ribadisce lo scopo del CARF MCAA di migliorare l'adempimento fiscale internazionale in relazione alle cripto-attività pertinenti. Chiarisce inoltre che l'applicazione del CARF MCAA può dipendere dal completamento positivo delle procedure legislative nazionali (ad esempio, l'approvazione parlamentare e/o un referendum) e ribadisce che la stipula del CARF MCAA è soggetta all'adesione delle Parti al principio della riservatezza, alle garanzie per la protezione dei dati e ad altre misure di tutela, ivi inclusa la limitazione dell'uso delle informazioni scambiate nella misura prevista dalla Convenzione.

Commentario alla sezione 1 relativa alle definizioni

Punto 1 – Definizioni

1. Il punto 1, lettera a) definisce le giurisdizioni delle Autorità competenti che hanno firmato il CARF MCAA e si riferisce a un Paese o a un territorio nei confronti del quale la Convenzione è in vigore (Convenzione originale) o applicabili (nel caso della Convenzione modificata) attraverso la ratifica o l'estensione territoriale.

2. La definizione di "Autorità competente" stabilita nel punto 1, lettera b) si riferisce alle persone e alle autorità elencate nell'Allegato B della Convenzione.

3. La definizione del termine "quadro per la comunicazione di informazioni in materia di cripto-attività" di cui al punto 1, lettera c), si riferisce al quadro internazionale per lo scambio automatico di informazioni relative alle cripto-attività (che include i Commentari) sviluppato dall'OCSE con i Paesi del G20.

4. È possibile che il CARF, comprese le modalità informatiche come lo schema XML, venga aggiornato periodicamente, via via che un numero maggiore di giurisdizioni lo attuerà e ne farà esperienza. Inoltre, nel contesto del CARF MCAA, le Autorità competenti possono firmare in date diverse e, a causa di ciò, il CARF potrebbe essere nel frattempo diventato oggetto di un aggiornamento. A questo proposito, e al fine di garantire che vi sia un'intesa sul fatto che tutte le giurisdizioni dovrebbero dare attuazione alla versione più recente del CARF in relazione ai prestatori di servizi per le cripto-attività con obbligo di comunicazione che sono soggetti agli obblighi di adeguata verifica in materia fiscale e di comunicazione nella loro giurisdizione, il quinto "considerando" afferma che " le leggi delle giurisdizioni devono essere modificate periodicamente alla luce degli aggiornamenti del Quadro per la comunicazione di informazioni in materia di cripto-attività e che, una volta che tali leggi di modifica siano state promulgate da una giurisdizione, il termine Quadro per la comunicazione di informazioni in materia di cripto-attività sarà inteso come facente riferimento alla versione aggiornata in relazione a tale giurisdizione".

5. La definizione del termine "Segretariato dell'organo di coordinamento" di cui al punto 1, lettera d), si riferisce al Segretariato dell'OCSE che, ai sensi dell'articolo 24, paragrafo 3 della Convenzione, fornisce supporto all'organo di coordinamento composto dai rappresentanti delle Autorità competenti delle Parti alla Convenzione.

6. Ai sensi del punto 1, lettera e), il CARF MCAA è un "Accordo applicabile" nei confronti di una qualsiasi delle due Autorità competenti se queste si sono incluse reciprocamente nell'elenco dei partner di scambio previsti (notifica ai sensi della sezione 7, punto 1), lettera g)) e se hanno soddisfatto le altre condizioni di cui alla sezione 7, punto 2. L'elenco delle Autorità competenti per le quali è applicabile il presente Accordo sarà pubblicato sul sito web dell'OCSE.

Punto 2 - Regola generale di interpretazione

7. Il punto 2 stabilisce la regola generale di interpretazione. La prima frase del punto 2 chiarisce che tutti i termini con iniziali maiuscole utilizzati nel CARF MCAA ma non definiti in esso devono essere interpretati in modo conforme al significato attribuito loro nel CARF.

8. La seconda frase del punto 2 stabilisce che, a meno che il contesto non richieda un'altra interpretazione o che le Autorità competenti non concordino un'interpretazione comune, qualsiasi termine non altrimenti definito nel CARF MCAA o nel Quadro per la comunicazione di informazioni in materia di cripto-attività assume il significato che gli viene attribuito in quel momento dalla legge della giurisdizione che applica il CARF MCAA. A questo proposito, qualsiasi significato attribuito ai sensi delle leggi in materia fiscale applicabili di tale giurisdizione prevarrà sul significato attribuito a tale termine da altre leggi di detta giurisdizione. Inoltre, nell'esaminare il contesto, le Autorità competenti dovrebbero considerare il Commentario sul quadro per la comunicazione di informazioni in materia di cripto-attività.

Commentario alla sezione 2 relativa allo Scambio di informazioni in relazione alle persone oggetto di comunicazione

1. Il punto 1 fornisce la base giuridica per lo scambio e sancisce che le informazioni saranno scambiate su base annuale. Le informazioni possono essere scambiate anche più frequentemente di una volta all'anno. Ad esempio, quando un'Autorità competente riceve dati rettificati da un prestatore di servizi per le cripto-attività con obbligo di comunicazione, tali informazioni saranno generalmente inviate all'altra Autorità competente quanto prima successivamente alla loro ricezione. Le informazioni oggetto di scambio sono quelle ottenute in virtù della sezione II del Quadro per la comunicazione di informazioni in materia di cripto-attività e sono ulteriormente specificate al punto 3.

2. Il punto 1 chiarisce inoltre che lo scambio di informazioni è soggetto alle norme di comunicazione e di adeguata verifica in materia fiscale del Quadro per la comunicazione di informazioni in materia di cripto-attività. Pertanto, laddove tali norme non richiedano la comunicazione, ad esempio, di un NIF o del luogo di nascita di una determinata persona oggetto di comunicazione, non sussiste nemmeno l'obbligo di scambiare tali informazioni.

3. Il punto 2 descrive i requisiti relativi alle giurisdizioni che hanno dichiarato di voler essere inserite nell'elenco delle giurisdizioni per le quali non sussiste reciprocità sulla base di una notifica ai sensi della sezione 7, punto 1, lettera b). Tali giurisdizioni invieranno, ma non riceveranno, le informazioni specificate nel punto 3. Al contrario, le giurisdizioni non inserite nell'elenco delle giurisdizioni per la quali non sussiste reciprocità riceveranno le informazioni di cui al punto 3 dalle giurisdizioni inserite nell'elenco, ma non le invieranno alle medesime.

4. Il punto 3 elenca le informazioni oggetto di scambio in relazione a ciascuna persona oggetto di comunicazione di un'altra giurisdizione. Per tutte le categorie di comunicazione ai sensi della sezione 2,

punto 3, lettera c), punto ii) fino al punto 3 , lettera c), punto ix), il Quadro per la comunicazione di informazioni in materia di cripto-attività richiede l'aggregazione, ossia la somma, di tutte le operazioni pertinenti attribuibili a ciascuna categoria di comunicazione per ciascun tipo di cripto-attività pertinente, nella forma convertita e valutata ai sensi delle parti D ed E della sezione II del Quadro per la comunicazione di informazioni in materia di cripto-attività e dei punti 33-41 del Commentario alla sezione II.

Commentario alla sezione 3 relativa ai tempi e alle modalità di scambio delle informazioni

Punto 1 – Tempi dello scambio di informazioni

1. Il punto 1 stabilisce che le informazioni di cui alla sezione 2 devono essere scambiate entro i nove mesi successivi al termine dell'anno civile a cui le informazioni si riferiscono. Il primo anno rispetto al quale vengono scambiate le informazioni è quello indicato dall'Autorità competente firmataria nella sua notifica ai sensi della sezione 7, punto 1, lettera a), in cui conferma che la propria giurisdizione è dotata della legislazione di attuazione richiesta. Il termine di nove mesi di cui al punto 1 è uno standard minimo e le giurisdizioni sono libere di procedere allo scambio prima dei termini prescritti.

2. Il punto 1 prevede inoltre che, a prescindere dall'anno che le Autorità competenti hanno indicato nella loro notifica ai sensi della sezione 7, punto 1), lettera a), come l'anno in cui avverrà il primo scambio, lo scambio di informazioni è richiesto solo in relazione a un anno civile se entrambe le giurisdizioni dispongono di una legislazione che dà attuazione al Quadro per la comunicazione di informazioni in materia di cripto-attività in relazione a tale anno civile. Una giurisdizione può tuttavia scegliere, nel rispetto delle proprie leggi nazionali, di scambiare le informazioni con un'altra giurisdizione in relazione a determinati anni (precedenti), se ha dato applicazione al Quadro per la comunicazione di informazioni in materia di cripto-attività e se il CARF MCAA è applicabile con l'Autorità competente di tale giurisdizione.

3. L'esempio che segue illustra l'applicazione dell'ultima frase del punto 1. Le giurisdizioni A e B hanno firmato il CARF MCAA. La giurisdizione A fornisce le proprie notifiche ai sensi della sezione 7, punto 1) il 7 giugno 2025, indicando di essere dotata di una legislazione applicabile che prevede l'obbligo di comunicazione per il 2026. La giurisdizione B fornisce le proprie notifiche il 1º novembre 2025, indicando di avere una legislazione applicabile che prevede l'obbligo di comunicazione per il 2027. In questo caso, l'ultima frase del punto 1 sarà applicata in modo tale che la giurisdizione A non sia sottoposta all'obbligo di scambiare informazioni in relazione al 2026. Entrambe le giurisdizioni A e B avranno l'obbligo di scambiare informazioni in relazione al 2027. Tuttavia, la giurisdizione A può scegliere, nel rispetto della propria legislazione nazionale, di inviare informazioni alla giurisdizione B in relazione al 2026 anche se la giurisdizione A non riceverà informazioni in relazione a detto anno.

Punti 2 e 3 - Modalità di utilizzo delle tecnologie d'informazione

Schema CARF e guida per l'utente

4. Il punto 2 prevede che le Autorità competenti si scambino automaticamente le informazioni descritte nella sezione 2 in uno schema comune in *Extensible Markup Language*, ovvero lo schema XML CARF.

Trasmissione dei dati, compresa la cifratura

5. Il punto 3 prevede che le Autorità competenti trasmettano le informazioni attraverso il Sistema comune di trasmissione dell'OCSE, che è il sistema di trasmissione protetta comunemente sviluppato e utilizzato dalle Autorità competenti di tutto il mondo per la trasmissione di informazioni fiscali riservate. Le

informazioni devono inoltre essere predisposte e cifrate in linea con i più recenti standard concordati a livello internazionale.

6. In alternativa, le Autorità competenti possono utilizzare un altro metodo per la trasmissione dei dati, come specificato da tali Autorità competenti nella loro notifica ai sensi della sezione 7, punto 1, lettera d). Qualsiasi metodo di trasmissione alternativo deve soddisfare standard di sicurezza, cifratura e preparazione dei file equivalenti a quelli applicabili al Sistema comune di trasmissione dell'OCSE, al fine di garantire la riservatezza e l'integrità dei dati durante l'intera trasmissione nonché assicurare che in nessun caso i dati siano resi disponibili o divulgati a persone non autorizzate né siano modificati o alterati in modo non autorizzato.

7. Un metodo di cifratura di uso comune per lo scambio di informazioni utilizza una chiave pubblica e una privata. La cifratura a chiave pubblica è in uso da alcuni decenni e consente alle parti di scambiare dati cifrati senza comunicare in anticipo una chiave segreta condivisa. La parte che invia le informazioni cripta il file di dati con una chiave pubblica e solo la parte ricevente possiede la chiave privata sicura che consente di decifrare i dati. Esistono standard per la lunghezza delle chiavi di crittografia in uso a livello internazionale che attestano un livello di sicurezza adeguato per i dati finanziari personali, sia attualmente che nel prossimo futuro, come ad esempio lo standard di crittografia avanzata (AES) 256.

Commentario alla sezione 4 relativa alla collaborazione ai fini della conformità e dell'applicazione

1. La sezione 4 definisce le aspettative in termini di collaborazione tra le Autorità competenti ai fini della conformità e dell'applicazione. Essa prevede che qualora un'Autorità competente abbia motivo di ritenere che un errore possa essere stato all'origine di una comunicazione di informazioni inesatte o incomplete o che un prestatore di servizi per le cripto-attività con obbligo di comunicazione non abbia rispettato gli obblighi applicabili, tale Autorità competente deve notificarlo all'altra Autorità competente. L'Autorità competente notificata è in seguito tenuta ad adottare tutte le misure previste dal proprio diritto nazionale per ovviare agli errori o alla non conformità oggetto della notifica. Ciò include i casi in cui una persona oggetto di comunicazione invoca i diritti dell'interessato per ottenere la correzione o la cancellazione dei dati errati. Prima di inviare una notifica formale, le Autorità competenti dovrebbero prendere in considerazione la possibilità di consultarsi informalmente sugli errori o sui casi di non conformità individuati. Si veda il Commentario alla sezione V del Quadro per la comunicazione di informazioni in materia di cripto-attività per quanto concerne le norme e le procedure amministrative di cui le giurisdizioni devono essere dotate al fine di garantire l'effettiva attuazione di detto quadro.

2. Qualsiasi notifica ai sensi della presente sezione deve indicare chiaramente l'errore o la non conformità e le ragioni per cui si suppone che essi siano occorsi. L'Autorità competente notificata deve fornire una risposta o un aggiornamento il prima possibile e non oltre 90 giorni di calendario dalla ricezione della notifica da parte dell'altra Autorità competente. Se la questione non è stata risolta, l'Autorità competente notificata deve fornire aggiornamenti all'altra Autorità competente ogni 90 giorni. Se, tuttavia, dopo aver esaminato e valutato la notifica in buona fede, l'Autorità competente notificata non concorda sul fatto che esista o sia esistito un errore o una non conformità, dovrebbe, non appena possibile, informare per iscritto l'altra Autorità competente di tale decisione e spiegarne le ragioni.

Commentario alla sezione 5 relativa alla riservatezza e alle garanzie per la protezione dei dati

1. La riservatezza delle informazioni sui contribuenti ha sempre costituito una pietra miliare dei sistemi fiscali e dello scambio internazionale di informazioni fiscali. Le giurisdizioni hanno l'obbligo legale

di garantire che le informazioni scambiate rimangano riservate e vengano utilizzate solo in conformità ai termini dell'accordo in virtù del quale sono state scambiate. Per avere fiducia nei loro sistemi fiscali e rispettare gli obblighi previsti dalla legge, i contribuenti devono sapere che le informazioni finanziarie non vengono divulgate in modo inappropriato, sia intenzionalmente che accidentalmente. I contribuenti e i governi daranno fiducia allo scambio internazionale solo qualora le informazioni scambiate vengano utilizzate e divulgate in conformità allo strumento che ne disciplina lo scambio. Si tratta non solo di disporre di un quadro giuridico, ma anche di sistemi e procedure atti a garantire che il medesimo sia rispettato nella prassi e che non sussista una divulgazione o un uso non autorizzato delle informazioni. La capacità di proteggere la riservatezza delle informazioni fiscali è anche il risultato di una "cultura dell'attenzione" all'interno di un'amministrazione fiscale che contempla l'intera gamma di sistemi, procedure e processi per garantire il rispetto del quadro giuridico nella prassi nonché la sicurezza e l'integrità delle informazioni nella gestione delle stesse. Con l'aumentare del livello di sofisticatezza di un'amministrazione fiscale, i processi e le pratiche di riservatezza devono tenere il passo per garantire che le informazioni scambiate rimangano riservate e vengano utilizzate in modo appropriato. A questo proposito, diverse giurisdizioni dispongono di norme specifiche sulla protezione dei dati personali e dei diritti dell'interessato, che si applicano anche alle informazioni dei contribuenti.

2. La sezione 5, insieme alla sezione 7 e alle dichiarazioni contenute nell'ottavo considerando del preambolo, riconoscono esplicitamente l'importanza della riservatezza e della protezione dei dati in relazione allo scambio automatico di informazioni ai sensi del CARF MCAA. Il Commentario a questa sezione esamina brevemente i punti 1 e 2, seguiti da una descrizione completa dell'approccio alla riservatezza e alla protezione dei dati in relazione al quadro per la comunicazione di informazioni in materia di cripto-attività.

Punto 1 - Riservatezza e protezione dei dati personali

3. Tutte le informazioni scambiate nell'ambito del CARF MCAA sono soggette alle norme in materia di riservatezza e alle altre salvaguardie previste dalla Convenzione. Ciò include le limitazioni relative alle finalità per cui le informazioni possono essere utilizzate e i limiti relativi ai destinatari di tali informazioni. In particolare, l'articolo 22 della Convenzione stabilisce che le informazioni scambiate con una Parte sono comunicate soltanto alle persone o alle autorità incaricate dell'accertamento, della riscossione o del recupero delle imposte, delle procedure o dei procedimenti penali, o delle decisioni su ricorsi concernenti tali imposte di tale Parte, unicamente per i fini ivi specificati.

4. Molte giurisdizioni dispongono di norme specifiche sulla protezione dei dati personali e sui diritti degli interessati che si applicano alle informazioni sui contribuenti. Ad esempio, norme speciali sulla protezione dei dati si applicano agli scambi di informazioni da parte degli Stati membri dell'UE (sia che lo scambio avvenga con un altro Stato membro dell'UE o con una giurisdizione terza).[1] Tali norme comprendono, tra l'altro, il diritto dell'interessato all'informazione, all'accesso, alla rettifica, al regresso nonché l'esistenza di un meccanismo di controllo per la tutela dei diritti dell'interessato.

5. L'articolo 22, paragrafo 1, della Convenzione modificata prevede che "Qualsiasi informazione ottenuta da una Parte [...] è considerata [...] nella misura necessaria per conseguire il giusto livello di protezione dei dati personali, conformemente alle eventuali clausole di salvaguardia specificate dalle disposizioni legislative nella giurisdizione che fornisce le informazioni". Alla luce di ciò, la sezione 5, punto 1, prevede che l'Autorità competente che fornisce le informazioni possa specificare tali clausole di salvaguardia in una notifica fornita ai sensi della sezione 7, punto 1, lettera e). L'Autorità competente che riceve le informazioni conferma nella notifica fornita ai sensi della sezione 7, punto 1, lettera g) (partner di scambio previsti) che la propria giurisdizione rispetta le condizioni specificate dalle Autorità competenti selezionate come partner di scambio previsti. L'Autorità competente che riceve le informazioni dovrà trattarle non solo in conformità alla propria legislazione, ma anche a ulteriori salvaguardie necessarie ad assicurare la protezione dei dati in virtù della legislazione dell'Autorità competente mittente. Tali

salvaguardie supplementari, come specificate dall'Autorità competente di invio, possono ad esempio riguardare l'accesso individuale a tali informazioni, la loro rettifica, cancellazione o il diritto di regresso. Potrebbe non essere necessario specificare le salvaguardie qualora l'Autorità competente che fornisce le informazioni sia soddisfatta del livello di protezione fornito ai dati ricevuti da parte dell'Autorità competente ricevente. In ogni caso, tali salvaguardie dovrebbero essere limitate a quanto necessario per garantire la protezione dei dati personali senza impedire o ritardare indebitamente l'effettivo scambio di informazioni, in considerazione del significativo interesse pubblico rivestito dallo scambio di informazioni in materia fiscale.

6. Gli strumenti di scambio di informazioni, compreso l'articolo 21 della Convenzione, prevedono in genere che le informazioni non debbano essere fornite a un'altra giurisdizione se la loro divulgazione è contraria all'ordine pubblico (*ordre public*) della giurisdizione che le fornisce. Sebbene sia raro che ciò si applichi nel contesto dello scambio di informazioni tra Autorità competenti, alcune giurisdizioni possono, ad esempio, richiedere alle proprie Autorità competenti di specificare che le informazioni fornite non possono essere utilizzate o divulgate in procedimenti che potrebbero portare all'imposizione e all'esecuzione della pena di morte o alla tortura o ad altre gravi violazioni dei diritti umani (ad esempio laddove le indagini fiscali sono motivate da persecuzioni politiche, razziali o religiose) qualora tale scambio possa pregiudicare l'ordine pubblico della giurisdizione che fornisce le informazioni.

Punto 2 - Violazione della riservatezza

7. È fondamentale garantire la costante riservatezza delle informazioni ricevute ai sensi dello strumento giuridico applicabile. La sezione 5, punto 2 stabilisce che, in caso di violazione della riservatezza o di qualsivoglia disfunzionamento delle salvaguardie nella giurisdizione (comprese le salvaguardie supplementari specificate dall'Autorità competente che fornisce le informazioni), l'Autorità competente di detta giurisdizione deve notificare immediatamente al Segretariato dell'organo di coordinamento tale violazione o disfunzionamento, comprese tutte le sanzioni o misure correttive conseguentemente applicate. Il contenuto di tale notifica deve rispettare a sua volta le norme di riservatezza e deve essere conforme al diritto interno della giurisdizione in cui è occorsa la violazione o il disfunzionamento. Inoltre, la sezione 7 prevede esplicitamente che la non conformità rispetto alle disposizioni in materia di riservatezza e di protezione dei dati (comprese le salvaguardie supplementari specificate dall'Autorità competente che fornisce le informazioni) sia considerata come non conformità significativa nonché una giustificazione per la sospensione immediata del CARF MCAA.

Garantire la costante conformità ai requisiti di riservatezza e di protezione dei dati

8. Al fine di stabilire le salvaguardie adeguate per proteggere le informazioni scambiate automaticamente sono imprescindibili tre elementi: i) un quadro giuridico che garantisca la riservatezza e l'uso appropriato delle informazioni scambiate in conformità con gli strumenti giuridici internazionali; ii) un sistema di gestione per la sicurezza delle informazioni (SGSI) che aderisca a standard riconosciuti a livello internazionale o alle migliori prassi; e iii) disposizioni e processi relativi all'applicazione che disciplinano le violazioni della riservatezza e l'uso improprio delle informazioni.

Quadro giuridico

9. Il quadro giuridico nazionale delle giurisdizioni dovrebbe includere disposizioni sufficienti a proteggere la riservatezza delle informazioni sui contribuenti, comprese le informazioni scambiate, e prevedere solo circostanze specifiche e limitate in cui tali informazioni possono essere divulgate e utilizzate; tali circostanze devono essere conformi, in relazione alle informazioni scambiate, ai termini dello strumento internazionale di scambio applicabile (bilaterale o multilaterale) in base al quale le informazioni sono state scambiate.

Sistema di Gestione per la Sicurezza delle Informazioni (GSI)

10. Le amministrazioni fiscali autorizzate ad accedere alle informazioni scambiate ai sensi dell'articolo 22, paragrafo 2 della Convenzione o di disposizioni equivalenti in altri accordi internazionali di scambio (di seguito "organizzazioni pertinenti") devono disporre di una politica e di sistemi di GSI volti a garantire che le informazioni possano essere utilizzate esclusivamente per gli scopi previsti e per impedirne la divulgazione a persone non autorizzate. Un sistema GSI è un insieme di accordi di *governance*, politiche, procedure e prassi che riguardano i rischi per la sicurezza delle informazioni, compresi i rischi legati alle tecnologie dell'informazione. I sistemi GSI devono aderire a standard o migliori prassi riconosciuti a livello internazionale.

11. Per standard o migliori prassi riconosciuti a livello internazionale si intende la "serie ISO/CEI 27000", pubblicata congiuntamente dall'Organizzazione internazionale per la standardizzazione (*International Standard Organisation* - ISO) e dalla Commissione elettrotecnica internazionale (*Electro-technical Commission* - IEC), che prevede le migliori prassi in materia di gestione della sicurezza delle informazioni, rischi e controlli nel contesto di un sistema di GSI globale.

12. Le organizzazioni pertinenti devono soddisfare i requisiti GSI nel loro sistema di GSI globale, nell'attuazione dei vari controlli di sicurezza e nel loro quadro operativo per testare l'efficacia di tali controlli, come segue.

13. Per quanto riguarda il sistema GSI complessivo, le organizzazioni pertinenti devono:

- mostrare una chiara comprensione del ciclo di vita delle informazioni scambiate all'interno dell'organizzazione e impegnarsi a garantirne la riservatezza e l'uso appropriato;
- gestire la sicurezza delle informazioni attraverso una politica scritta sulla sicurezza delle informazioni facente parte di un quadro generale di sicurezza che definisca chiaramente i ruoli e le competenze in materia di sicurezza, di cui sia responsabile l'alta dirigenza e che sia costantemente aggiornato;
- trattare la sicurezza delle informazioni, compresa la tecnologia, attraverso adeguati accordi operativi e come parte integrante della gestione dei processi aziendali pertinenti;
- gestire sistematicamente i rischi per la sicurezza delle proprie informazioni, tenendo conto delle minacce, delle vulnerabilità e degli impatti; e
- disporre di disposizioni adeguate a gestire e mantenere la continuità operativa.

14. Per quanto riguarda i controlli sulle risorse umane, le organizzazioni pertinenti devono:

- garantire che i ruoli e le responsabilità dei dipendenti e dei contraenti in materia di sicurezza siano definiti, documentati e chiaramente comunicati sotto il profilo dell'impiego, nonché regolarmente rivisti in conformità con la politica di sicurezza delle informazioni (ciò dovrebbe includere accordi di riservatezza e non divulgazione);
- effettuare controlli dei precedenti personali e un'adeguata verifica di tutti i candidati all'assunzione, dei dipendenti e dei contraenti, in conformità alle migliori prassi accettate e ai rischi percepiti;
- garantire che tutti i dipendenti e i contraenti siano regolarmente formati, sensibilizzati e aggiornati in materia di sicurezza, e che i dipendenti e i contraenti che ricoprono ruoli sensibili ricevano indicazioni aggiuntive per la gestione di materiale più sensibile;
- garantire che i dipendenti applichino le politiche e le procedure di sicurezza; e
- disporre di politiche e processi per le risorse umane relativi alla cessazione del rapporto di lavoro che proteggano le informazioni sensibili.

15. Per quanto riguarda i controlli degli accessi fisici e logici, le organizzazioni pertinenti devono:

- disporre di una politica di controllo degli accessi fisici di cui sia responsabile l'alta dirigenza;
- proteggere adeguatamente i locali fisici e disporre di perimetri di sicurezza interni ed esterni adeguatamente definiti;
- disporre di una politica di controllo degli accessi logici di cui sia responsabile l'alta dirigenza e basata sui principi della "necessità di sapere" e dell'"accesso di minimo privilegio "; e
- disporre di politiche, di processi e procedure, di cui sia responsabile l'alta dirigenza e non solo della funzione informatica dell'organizzazione, che disciplinino l'accesso logico, di processi efficaci per le attività di messa a disposizione e di revisione dell'accesso logico nonché per l'identificazione e l'autenticazione degli utenti.

16. Per quanto riguarda la sicurezza dei sistemi informatici, le organizzazioni pertinenti devono:

- fare della sicurezza una parte integrante dell'erogazione di servizi tecnologici, disporre di un piano di sicurezza per le applicazioni e armonizzare i propri sistemi con la sicurezza;
- attuare una gamma adeguata di controlli di sicurezza;
- gestire adeguatamente le proprie attività;
- gestire in modo appropriato la fornitura di servizi da parte dei fornitori; e
- garantire la continuità dei servizi informatici sulla base di accordi sul livello del servizio.

17. Per quanto riguarda la protezione delle informazioni, le organizzazioni pertinenti devono:

- gestire efficacemente le informazioni in conformità a una serie di politiche e procedure per tutto il ciclo di vita della gestione delle informazioni (compresi la denominazione, la classificazione, il trattamento, l'archiviazione, il monitoraggio, la revisione e la distruzione dei documenti, nonché i dispositivi e i supporti che contengono le informazioni); e
- disporre di processi per le informazioni ricevute da altre Autorità competenti, al fine di garantire il rispetto degli obblighi previsti dagli accordi internazionali di scambio, con l'ulteriore fine di evitare la commistione con altre informazioni.

18. Per quanto riguarda il quadro di gestione delle operazioni, tra cui la gestione degli incidenti, la gestione delle modifiche, il monitoraggio e l'audit, le organizzazioni pertinenti devono:

- essere consapevoli dei controlli che proteggono le informazioni scambiate e disporre di piani adeguati a gestirli;
- disporre di adeguati dispositivi di monitoraggio e registrazione, anche per rilevare accessi, usi o divulgazioni non autorizzati delle informazioni;
- analizzare e reagire ai rischi per la sicurezza;
- disporre di processi e procedure per l'identificazione e la gestione delle vulnerabilità note;
- disporre di un processo di gestione delle modifiche dotato di sicurezza integrata;
- disporre di un sistema di gestione degli incidenti che contempli tutti i tipi di incidenti di sicurezza; e
- disporre di funzioni di audit interno ed esterno.

Disposizioni e processi relativi all'applicazione contro le violazioni della riservatezza

19. Il quadro giuridico delle giurisdizioni deve inoltre prevedere sanzioni per la non conformità rispetto alle disposizioni in materia di riservatezza e di protezione dei dati per garantirne il rispetto. Il quadro giuridico e il quadro del GSI devono essere rafforzati da norme amministrative, risorse e procedure adeguate, come la capacità di gestire le violazioni sospette o effettive e di adottare misure correttive. Dovrebbero inoltre essere apportate modifiche ai processi per mitigare il rischio e prevenire future violazioni.

20. In particolare, il quadro giuridico nazionale delle giurisdizioni dovrebbe consentire l'imposizione di sanzioni adeguate e appropriate rispetto alla divulgazione o all'uso improprio delle informazioni sui contribuenti, comprese le informazioni scambiate, che contemplino altresì sanzioni amministrative, civili e penali.

21. Inoltre, le giurisdizioni dovrebbero:

- disporre di processi da seguire in caso di accesso, uso o divulgazione non autorizzati, sospetti o effettivi, che garantiscano la segnalazione e l'investigazione di tali infrazioni;
- avvalendosi di risorse amministrative, processi e procedure adeguate, garantire che vengano adottate misure correttive laddove siano stati individuati problemi effettivi, con l'applicazione pratica di sanzioni o penalità adeguate nei confronti di dipendenti, contraenti e altre persone che violano le norme di riservatezza, le politiche o le procedure di sicurezza, al fine di dissuadere altri dal commettere violazioni simili;
- applicare processi per notificare alle altre Autorità competenti le violazioni della riservatezza o il disfunzionamento delle salvaguardie, nonché le sanzioni e le misure correttive conseguentemente applicate; e
- rivedere i processi di monitoraggio e applicazione delle sanzioni in risposta alla non conformità, prevedendo l'alta dirigenza quale garante dell'attuazione delle raccomandazioni per il cambiamento.

Commentario alla sezione 6 relativa alle consultazioni e alle modifiche

Punto 1 – Consultazioni

1. Questo punto prevede che, in caso di problemi relativi all'applicazione o all'interpretazione del CARF MCAA, l'Autorità competente possa richiedere consultazioni per definire misure atte a garantire la corretta applicazione dell'accordo. Le consultazioni possono essere tenute altresì per analizzare la qualità delle informazioni ricevute.

2. Le Autorità competenti possono comunicare tra loro al fine di raggiungere un accordo sulle misure atte a garantire il rispetto del CARF MCAA. Il Segretariato dell'organo di coordinamento comunicherà a tutte le Autorità competenti, comprese quelle che non hanno partecipato alla consultazione, tutte le misure sviluppate per garantire il rispetto del CARF MCAA.

Articolo 2 – Modifiche

3. Questo paragrafo chiarisce che il CARF MCAA può essere modificato mediante accordo scritto delle Autorità competenti. Salvo diverso accordo tra le Autorità competenti, la modifica ha effetto il primo giorno del mese successivo allo scadere di un periodo di un mese dopo la data dell'ultima firma apposta a detto accordo scritto.

Commentario alla sezione 7 relativa ai termini generali

Punto 1 – Notifiche

1. Il punto 1 descrive le notifiche che, al momento della firma del CARF MCAA o appena possibile successivamente, un'Autorità competente deve fornire al Segretariato dell'organo di coordinamento prima che il CARF MCAA possa essere applicato nei confronti di un'altra Autorità competente:

- la notifica di cui al punto 1, lettera a) conferma che la giurisdizione dispone delle leggi necessarie per attuare il Quadro per la comunicazione di informazioni in materia di cripto-attività, e specifica le relative date di entrata in vigore di tale legislazione. Ciò potrebbe includere la specificazione di eventuali condizioni nelle procedure legislative nazionali che potrebbero richiedere l'applicazione provvisoria del CARF MCAA per un periodo limitato. Quando si specifica tale applicazione provvisoria, la notifica dovrebbe indicare lo stato di avanzamento delle procedure legislative nazionali, le ragioni dell'applicazione provvisoria e il periodo di tempo, che in ogni caso non dovrebbe estendersi oltre la fine del primo periodo di riferimento. La notifica dovrebbe fornire garanzie circa la capacità della legislazione della giurisdizione di garantire l'adempimento degli obblighi di adeguata verifica in materia fiscale e di comunicazione del Quadro per la comunicazione di informazioni in materia di cripto-attività nei confronti di tutti i prestatori di servizi per le cripto-attività con obbligo di comunicazione che sono soggetti a detti obblighi nella giurisdizione in virtù della sezione I di detto Quadro, in particolare includendo riferimenti specifici alla legislazione applicabile che garantisce l'adempimento di tali obblighi;
- la notifica di cui al punto 1, lettera b) conferma l'intenzione da parte della giurisdizione di essere inserita nell'elenco delle giurisdizioni per le quali sussiste reciprocità o nell'elenco delle giurisdizioni per le quali non sussiste reciprocità (ad esempio perché la giurisdizione non dispone di un sistema di imposizione diretta o perché l'Autorità competente della giurisdizione non assicura un livello adeguato di riservatezza e protezione dei dati). Una giurisdizione per la quale non sussiste reciprocità è tenuta a inviare le informazioni previste dalla sezione 2, ma non riceverà informazioni da altre Autorità competenti. Un'Autorità competente deve depositare la propria notifica di intenzione di essere inserita nell'elenco delle giurisdizioni per cui non sussiste la reciprocità, anche qualora quest'ultima sia solo temporanea (ad esempio, in attesa di una valutazione delle garanzie di riservatezza e in materia di dati);
- La notifica di cui al punto 1, lettera c), prevede una dichiarazione da parte dell'Autorità competente volta a richiedere il consenso delle altre Autorità competenti a utilizzare le informazioni ricevute in virtù del CARF MCAA per l'accertamento, la riscossione o il recupero delle imposte, delle procedure o dei procedimenti penali concernenti tali imposte, o delle decisioni sui ricorsi presentati per tali imposte per le quali la propria giurisdizione ha espresso una riserva ai sensi dell'articolo 30, paragrafo 1, lettera a) della Convenzione. L'Autorità competente che richiede le informazioni deve specificare tali imposte e confermare che il relativo utilizzo avverrà secondo i termini della Convenzione. L'altra Autorità competente deve acconsentire esplicitamente a tale utilizzo nell'elencare l'Autorità competente richiedente quale partner di scambio previsto nella notifica fornita ai sensi del punto 1, lettera g);
- nella quarta notifica di cui al punto 1, lettera d), l'Autorità competente deve indicare se intende avvalersi di metodi di trasmissione e di cifratura diversi dal sistema comune di trasmissione dell'OCSE e dei relativi metodi di preparazione e di cifratura dei file;
- la notifica di cui al punto 1, lettera e), stabilisce che la giurisdizione deve specificare eventuali obblighi in materia di protezione dei dati personali che devono essere rispettati nella giurisdizione destinataria in relazione alle informazioni inviate alle Autorità competenti di tali giurisdizioni, oltre agli obblighi in materia di riservatezza e limitazione dell'uso contenuti nell'articolo 22 della Convenzione. Ciò consente all'Autorità competente di invio di subordinare l'invio di qualsiasi informazione alla conferma dell'esistenza di determinate salvaguardie nella giurisdizione destinataria. L'altra Autorità competente deve accettare esplicitamente tali salvaguardie nell'elencare l'Autorità competente di invio come partner previsto per lo scambio nella notifica fornita ai sensi del punto 1, lettera g). In alternativa, nell'ambito di tale notifica, un'Autorità competente può anche limitarsi a indicare che non intende fornire ulteriori specifiche in merito alla protezione dei dati;

- la notifica di cui al punto 1, lettera f), richiede che le giurisdizioni confermino di aver adottato misure adeguate a garantire il rispetto degli standard di riservatezza e protezione dei dati, come discusso nella sezione 5. La conferma può avvenire facendo riferimento al relativo Rapporto sulla riservatezza e sulle garanzie in materia di dati per le giurisdizioni adottato dal Forum globale sulla trasparenza e lo scambio di informazioni a fini fiscali;
- infine, nella notifica di cui al punto 1, lettera g), l'Autorità competente dovrebbe includere un elenco delle giurisdizioni delle Autorità competenti rispetto alle quali intende applicare il presente accordo, seguendo le procedure legislative nazionali per l'entrata in vigore (se del caso). Includendo una giurisdizione in tale elenco, l'Autorità competente accetta anche di conformarsi agli obblighi in materia di protezione dei dati notificati dall'Autorità competente di tale giurisdizione ai sensi del punto 1, lettera e). Inoltre, se del caso, l'Autorità competente può specificare in tale notifica se acconsente all'uso delle informazioni oggetto di scambio con l'Autorità competente di un'altra giurisdizione per l'amministrazione del recupero delle imposte di cui alla notifica ai sensi del punto 1, lettera c).

2. Oltre alle notifiche di cui sopra, il punto 1 stabilisce che le Autorità competenti devono comunicare tempestivamente al Segretariato dell'organo di coordinamento ogni successiva modifica da apportare alle notifiche di cui sopra.

Punto 2 – Entrata in vigore

3. Il punto 2 stabilisce che uno specifico rapporto di scambio bilaterale viene attivato ed entra in vigore alla data in cui la seconda delle due Autorità competenti fornisce tutte le notifiche richieste ai sensi del punto 1 al Segretariato dell'organo di coordinamento e ha elencato la giurisdizione dell'altra Autorità competente ai sensi della sezione 7, punto 1, lettera g).

Punti 3 e 4 – Ruolo del Segretariato dell'organo di coordinamento

4. Il punto 3 chiarisce che il Segretariato dell'organo di coordinamento conserverà un elenco delle Autorità competenti che hanno firmato il CARF MCAAA, nonché tra quali Autorità competenti è applicato l'Accordo. Tali informazioni sono pubblicate sul sito web dell'OCSE.

5. Il punto 4 spiega inoltre che il Segretariato dell'organo di coordinamento pubblicherà sul sito web dell'OCSE le notifiche presentate ai sensi della sezione 7, punto 1, lettera a) (che conferma che la giurisdizione dispone delle leggi necessarie), punto 1, lettera b) (che conferma l'eventuale volontà della giurisdizione di essere inserita nell'elenco delle giurisdizioni per le quali non sussiste reciprocità) e punto 1, lettera e) (che specifica i requisiti di protezione dei dati). Il Segretariato dell'organo di coordinamento conserverà altresì le informazioni fornite dalle Autorità competenti ai sensi della sezione 7, punto 1, lettere c), d), f) e g). Tali informazioni, tuttavia, non saranno pubblicate sul sito web dell'OCSE e saranno rese disponibili solo ai firmatari del CARF MCAA.

Punto 5 – Sospensione

6. Il punto 5 fornisce dettagli sulla possibilità per un'Autorità competente di sospendere il CARF MCAA in relazione a un'altra Autorità competente quando ha determinato che esiste o è esistita una non conformità significativa da parte di tale altra Autorità competente. Ove possibile, le Autorità competenti devono cercare di risolvere eventuali questioni di non conformità, anche di grave entità, prima di emettere una notifica di reciproca sospensione del CARF MCAA.

7. Per sospendere il CARF MCAA, un'Autorità competente deve notificare per iscritto all'altra Autorità competente la propria intenzione di sospendere il CARF MCAA con la suddetta Autorità competente. La

notifica deve, ove possibile, indicare le ragioni della sospensione e le misure (da adottare) per risolvere la questione. La sospensione avrà effetto immediato.

8. L'Autorità competente notificata deve adottare quanto prima le misure necessarie per risolvere la grave inadempienza. Non appena quest'ultima è risolta, l'Autorità competente notificata deve informare la controparte. Una volta risolta con successo la questione, l'Autorità competente che ha emesso la notifica di sospensione deve confermare per iscritto all'Autorità competente notificata che il CARF MCAA non risulta più sospeso e che lo scambio di informazioni deve riprendere il prima possibile.

9. Il punto 5 stabilisce che una non conformità significativa include, tra l'altro:

- l'inosservanza delle disposizioni del CARF MCAA relative alla riservatezza o alla protezione dei dati, ad esempio relativamente a un utilizzo delle informazioni per scopi non autorizzati dal CARF MCAA o dalla Convenzione nonché a una modifica della legislazione nazionale suscettibile di compromettere la riservatezza delle informazioni; oppure
- la mancata comunicazione di informazioni tempestive o adeguate da parte dell'Autorità competente, come previsto dal CARF MCAA.

10. Durante il periodo di sospensione, tutte le informazioni ricevute in precedenza ai sensi del CARF MCAA rimarranno riservate e soggette ai termini della sezione 5 del CARF MCAA, comprese le eventuali garanzie aggiuntive in materia di dati specificate dall'Autorità competente mittente.

Punto 6 - Disattivazione e denuncia

11. Ai sensi del punto 6, un'Autorità competente può disattivare un particolare rapporto di scambio nell'ambito del CARF MCAA o denunciare completamente il CARF MCAA. In entrambi i casi l'Autorità competente deve darne comunicazione scritta al Segretariato dell'organo di coordinamento. La disattivazione o la denuncia ha effetto il primo giorno del mese successivo allo scadere di un periodo di 12 mesi dopo la data di ricezione della notifica. In circostanze in cui ciò sia reso necessario (ad esempio, a causa di procedure legislative nazionali o di una sentenza del tribunale), l'Autorità competente che disattiva uno o più rapporti di scambio nell'ambito del CARF MCAA o che cessa la sua partecipazione allo stesso, può discostarsi dal periodo predefinito di 12 mesi e specificare un altro periodo.

12. La cessazione della partecipazione di una giurisdizione alla Convenzione comporterà la cessazione automatica del CARF MCAA nei confronti di detta giurisdizione. Conseguentemente, in tali circostanze, il CARF MCAA non dovrà essere denunciato separatamente.

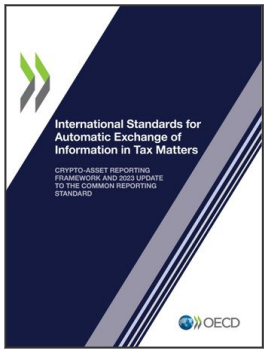
13. Il punto 6 chiarisce che in caso di disattivazione o cessazione, tutte le informazioni ricevute in precedenza ai sensi del CARF MCAA rimarranno riservate e soggette ai termini della sezione 5, comprese le eventuali garanzie aggiuntive in materia di dati specificate dall'Autorità competente mittente.

Commentario alla sezione 8 relativa al Segretariato dell'organo di coordinamento

1. La sezione 8 chiarisce che, salvo diverse indicazioni del CARF MCAA, il Segretariato dell'organo di coordinamento notificherà a tutte le Autorità competenti le notifiche ricevute ai sensi del CARF MCAA. La sezione 8 chiarisce inoltre che l'organo di coordinamento notificherà a tutti i firmatari del CARF MCAA la firma di una nuova Autorità competente.

Nota

[1] Cfr. Regolamento generale sulla protezione dei dati dell'UE (RGPD) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:02016R0679-20160504.



From:

International Standards for Automatic Exchange of Information in Tax Matters

Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard

Access the complete publication at:

https://doi.org/10.1787/896d79d1-en

Please cite this chapter as:

OECD (2024), "Commentario all'Accordo multilaterale delle Autorità competenti", in *International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/42789ca5-it

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at http://www.oecd.org/termsandconditions.

OECD