FIVERS

Aggiornamento
Data protection, AI, IT and IP

n. 2 / 2025

DATA PROTECTION.

20 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: adottato il rapporto sul CEF 2024 (Coordinated Enforcement Framework) sullo stato di attuazione del diritto di accesso da parte dei Titolari del trattamento in UE.

---

17 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: pubblicate le Linee Guida 1/2025 sulla pseudonimizzazione, in consultazione pubblica fino al 28 febbraio 2025.

---

16 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: pubblicato un rapporto di sintesi sulle decisioni delle Autorità data protection in materia di diritto di accesso in sede di one-stop-shop (OSS).

---

16 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: agenda dei lavori e nuovi provvedimenti.

---

14 Gennaio 2024 – CNIL: come impostare le app mobili in conformità alle norme sulla protezione dei dati personali.

---

9 Gennaio 2024 – Corte di Giustizia UE: chiarimenti interpretativi sulla nozione di "richieste eccessive" ai sensi dell'articolo 57, comma 4, del GDPR.

---

9 Gennaio 2024 – Corte di Giustizia UE: l'identità di genere del cliente non è un dato necessario per l'acquisto di un titolo di trasporto.

INTELLIGENZA ARTIFICIALE.

7 Gennaio 2025 – I principali trend e sviluppi attesi nel 2025 per l'Intelligenza Artificiale.

MERCATI DIGITALI

17 Gennaio 2025 – Il Regolamento DORA sulla resilienza operativa digitale è pianamente applicabile.

---

16 Gennaio 2025 – In Gazzetta dell'UE la strategia europea in materia di giustizia elettronica 2024-2028.

INFORMATION TECHNOLOGY

10 Gennaio 2025 – In vigore dal 25 Gennaio 2025 le nuove norme per lo svolgimento della mediazione civile e commerciale con modalità telematiche.

DATA PROTECTION

20 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: adottato il rapporto sul CEF 2024 (Coordinated Enforcement Framework) sullo stato di attuazione del diritto di accesso da parte dei Titolari del trattamento in UE.

Il Comitato europeo per la protezione dei dati (EDPB) ha adottato la **relazione sull'attuazione del diritto di accesso da parte dei titolari del trattamento** che sintetizza i risultati di una serie di azioni nazionali coordinate condotte nel 2024 nell'ambito del cosiddetto CEF (*Coordinated Enforcement Framework*)**,** un'azione chiave dell'EDPB nell'ambito della sua strategia 2024-2027 volta a razionalizzare l'applicazione e la cooperazione tra le autorità di protezione dei dati. Nel corso del 2024, trenta autorità di protezione dei dati in tutta Europa hanno avviato indagini coordinate sul rispetto del diritto di accesso da parte dei titolari del trattamento, avviando indagini formali e richieste di informazioni presso 1.185 titolari del trattamento, costituiti da piccole e medie imprese (PMI), grandi aziende attive in diversi settori e settori, nonché da vari tipi di enti pubblici

I risultati riassunti nel rapporto suggeriscono che, se è diffusa la consapevolezza dell'importanza di tale diritto, è però necessaria una maggiore sensibilizzazione in merito alle *Linee Guida 1/2022 sul diritto di accesso* che l'EDPB ha adottato. Importanti le aree di criticità che l'EDPB ha individuato in materia di ostacolo alla piena attuazione del diritto di accesso: dalla mancanza di procedure interne documentate per gestire le richieste di accesso ad interpretazioni incoerenti ed eccessive dei limiti al diritto di accesso; fino agli ostacoli spesso incontrati dagli interessati a causa di requisiti formali frapposti dal titolare (come la richiesta di fornire un numero eccessivo di documenti di identificazione). Per ogni area critica la relazione fornisce un elenco di raccomandazioni non vincolanti che devono essere prese in considerazione dai titolari del trattamento e dalle autorità di protezione dei dati.

Nonostante le criticità esistenti, due terzi delle autorità di protezione dei dati partecipanti hanno comunque valutato il livello di conformità dei titolari del trattamento che hanno risposto per quanto riguarda il diritto di accesso da "medio" a "alto". Un fattore importante che ha avuto un impatto sul livello di conformità è stato il volume di richieste di accesso ricevute dai titolari del trattamento, nonché le dimensioni dell'organizzazione. Più specificamente, i titolari del trattamento di grandi dimensioni hanno mostrato un livello di conformità più elevato rispetto alle organizzazioni di piccole dimensioni e con meno risorse.

I risultati positivi in termini di buone pratiche sono stati osservati in numerosi Stati UE, come l'adozione di sistemi self-service che consentono alle persone di scaricare autonomamente i propri dati personali in pochi clic e in qualsiasi momento.

Il CEF 2025 (*Coordinated Enforcement Framework*) riguarderà l **l'attuazione del diritto alla cancellazione**.

---

17 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: pubblicate le Linee Guida 1/2025 sulla pseudonimizzazione, in consultazione pubblica fino al 28 febbraio 2025.

Il Comitato europeo per la protezione dei dati (EDPB) ha pubblicato le Linee guida 01/2025 sulla pseudonimizzazione per la consultazione pubblica.

Ribandendo la definizione di "*pseudonimizzazione*" contenuta nell'articolo 4 del GDPR, l'EDPB ha ricordato che la pseudonimizzazione può essere parzialmente o completamente invertita, rendendo nuovamente identificativo (e dunque "*personale*") il dato riferito alla persona fisica. Ciò può avvenire per associazione, collegando i dati pseudonimizzati ai dati originali o risalendo ai dati identificativi originali mediante l'utilizzo di informazioni aggiuntive conservate dal titolare del trattamento a tal fine.

Inoltre, le Linee Guida 1/2025 evidenziano, tra l'altro, che:

- la pseudonimizzazione può aiutare a soddisfare i requisiti di protezione dei dati, come la protezione dei dati fin dalla progettazione e per impostazione predefinita (*privacy by design*), la sicurezza e le misure supplementari per i trasferimenti internazionali di dati personali;

- in caso di trasmissione a terzi, il titolare del trattamento deve valutare se esiste ancora la riduzione del rischio ottenuta mediante pseudonimizzazione per il trattamento interno;
- il titolare del trattamento deve informare gli interessati sui processi di pseudonimizzazione che riguardano i loro dati personali e su come tali dati possono essere utilizzati per identificarli;
- qualsiasi violazione della sicurezza che porti ad una sorta di reverse engineering del dato e alla re-identificazione costituisce una violazione dei dati personali (*data breach*).

Quanto alle misure tecniche e alle garanzie per la pseudonimizzazione, l'EDPB ha sottolineato che per implementare la pseudonimizzazione, i titolari del trattamento dovrebbero:

- determinare gli obiettivi che intendono raggiungere con questa misura, per definire il dominio della pseudonimizzazione;
- decidere quali dati devono essere trattati; e
- stabilire determinate informazioni, come ad esempio quali attributi verranno pseudonimizzati, il metodo di pseudonimizzazione da utilizzare e chi lo eseguirà e lo memorizzerà.

Sarà possibile partecipare alla consultazione pubblica fino al 28 febbraio 2025.

---

16 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: pubblicato un rapporto di sintesi sulle decisioni delle Autorità data protection in materia di diritto di accesso in sede di one-stop-shop (OSS).

Il 16 gennaio 2025, il Comitato europeo per la protezione dei dati (EDPB) ha pubblicato un rapporto di sintesi sul diritto di accesso ai sensi dell'articolo 15 del Regolamento generale sulla protezione dei dati (GDPR) nell'ambito delle decisioni adottate in sede di applicazione del meccanismo di *one-stop-shop* (OSS) (in base al quale, se un'organizzazione tratta dati personali in più di uno Stato membro dell'UE, non è necessario che essa interagisca con tutte le autorità di protezione dei dati dei paesi in cui opera, individuandosi un'unica autorità di controllo principale - la Lead Supervisory Authority, LSA - che funge da punto di contatto centrale).

Dall'entrata in vigore del GDPR le autorità di protezione dei dati hanno collaborato strettamente per adottare un numero crescente di decisioni a sportello unico sul diritto di accesso, come dimostrato dall'elevato volume di decisioni disponibili nel registro dell'EDPB in materia. Il rapporto che sintetizza i casi *one-stop-shop* tiene presente sia linee guida dell'EDPB 01/2022 sui diritti degli interessati - Diritto di accesso, che le rilevanti sentenze della Corte di Giustizia UE. Fornisce – inoltre - esempi utili sull'esercizio del diritto di accesso in vari contesti (es: in caso di profili o account falsi che si spacciano per interessati) ed evidenzia le modalità con le quali le autorità di protezione dei dati interpretano le diverse componenti del diritto di accesso nei diversi casi.

---

16 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: agenda dei lavori e nuovi provvedimenti.

L'agenda dei lavori della prossima sessione del Comitato europeo per la protezione dei dati personali, prevista il 16 gennaio, prefigura interessanti novità. Tra i temi in discussione per la prossima adozione dei relativi provvedimenti vi sono: le linee guida sulla pseudonimizzazione, l'aggiornamento delle linee Guida operative per i DPO, il position paper sull'interrelazione tra diritto della concorrenza e protezione dei dati (penso anche alle recenti sentenze della Corte di Giustizia UE in merito ai rapporti tra relative autorità antitrust e data protection e al perimetro del potere di intervento nei rispettivi campi), fino ai risultati del CEF 2024, come è noto relativo al diritto di accesso.

---

14 Gennaio 2024 – CNIL: come impostare le app mobili in conformità alle norme sulla protezione dei dati personali.

L'autorità francese per la protezione dei dati (CNIL) ha annunciato la pubblicazione di raccomandazioni sulla privacy per le app mobili. Le raccomandazioni evidenziano come le autorizzazioni di accesso possano essere implementate nel contesto delle app mobili.

Le raccomandazioni sottolineano che le autorizzazioni tecniche devono essere distinte dalle richieste di consenso. Gli utenti devono essere in grado di capire, accettando o rifiutando le autorizzazioni, quali dati stanno condividendo con le app. Ad esempio, l'accesso alla posizione è esente dal consenso per il funzionamento stesso di un'app di navigazione, poiché i dati sono necessari per un servizio. Inoltre, anche quando è richiesto il consenso, non sempre una semplice richiesta di autorizzazione implica un consenso libero, specifico, informato e univoco ai sensi del GDPR.

Le raccomandazioni includono altresì le *best practice* per i fornitori di sistemi operativi nell'implementazione di un sistema di autorizzazioni, che dovrebbe consentire ai fornitori di sistemi operativi di scegliere:

- il grado di precisione dei dati forniti a seconda della finalità perseguita (es. localizzazione più o meno precisa);
- l'ambito materiale dell'autorizzazione (ad es. l'accesso alle foto selezionate piuttosto che alla galleria multimediale complessiva); e
- la durata durante la quale viene concessa l'autorizzazione (ad esempio, attivazione una tantum dell'autorizzazione o per una durata predeterminata).

Infine, i titolari del trattamento dei dati dovrebbero determinare se l'elaborazione collegata alle autorizzazioni comporta operazioni di lettura/scrittura che richiedono il consenso dell'utente. In questo caso specifico, l'implementazione di una piattaforma di gestione del consenso potrebbe essere necessaria per l'aggiunta di una richiesta di autorizzazione tecnica.

---

9 Gennaio 2024 – Corte di Giustizia UE: chiarimenti interpretativi sulla nozione di "richieste eccessive" ai sensi dell'articolo 57, comma 4, del GDPR.

L'articolo 57, comma 4, del Regolamento 679/2016 ("GDPR") prevede che l'autorità di controllo può addebitare un contributo spese ragionevole basato sui costi amministrativi o rifiutarsi di soddisfare le richieste dei soggetti che a detta autorità si rivolgono (anche in sede di presentazione di reclamo o di istanze di accesso) qualora le richieste siano manifestamente infondate o eccessive, in particolare per il carattere ripetitivo, spettando all'autorità di controllo dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Max Schrems, noto attività austriaco, aveva presentato alla autorità privacy austriaca (DSB) 77 reclami - in un periodo di circa 20 mesi - in merito al rifiuto di un noto social network di riscontrare le sue istanze di accesso. Reclami respinti dall'autorità privacy austriaca in quanto ritenuti eccessivi per il loro numero.

La Corte di Giustizia dell'Unione Europea (CGUE) si è pronunciata sulla causa C-416/23, affermando che le richieste di accesso "eccessive" ai sensi del GDPR non possono essere considerate tali solo per il loro numero. La CGUE ha chiarito in primo luogo che, ai sensi dell'articolo 57, paragrafo 4, del GDPR, il termine "richiesta" comprende anche i reclami ai sensi dell'art. 77 del GDPR. Inoltre, le richieste non possono essere qualificate «eccessive», ai sensi dell'articolo 57, paragrafo 4 del GDPR unicamente in ragione del loro numero nel corso di un periodo determinato, dato che l'esercizio della facoltà prevista dalla medesima disposizione è subordinato alla dimostrazione, da parte dell'autorità di controllo, dell'esistenza di un intento abusivo della persona che ha presentato dette richieste. Infine, quando viene posta di fronte a richieste eccessive, un'autorità di controllo può scegliere, con decisione motivata, tra addebitare un contributo spese ragionevole basato sui costi amministrativi o rifiutarsi di soddisfare la richiesta, tenendo conto di tutte le circostanze pertinenti e assicurandosi che l'opzione prescelta sia appropriata, necessaria e proporzionata.

---

9 Gennaio 2024 – Corte di Giustizia UE: l'identità di genere del cliente non è un dato necessario per l'acquisto di un titolo di trasporto.

L'associazione Mousse ha contestato dinanzi all'autorità francese per la protezione dei dati personali (la CNIL) la prassi dell'impresa ferroviaria francese SNCF Connect che obbliga sistematicamente i suoi clienti a indicare il loro appellativo («Signore» o «Signora») al momento dell'acquisto di titoli di trasporto online. Tale associazione ritiene che detto obbligo violi il regolamento generale sulla protezione dei dati (RGPD), in particolare sotto il profilo del principio di minimizzazione dei dati, in quanto l'indicazione dell'appellativo, che corrisponde a un'identità di genere, non sembra essere necessaria per l'acquisto di un titolo di trasporto ferroviario. Nel 2021 la CNIL ha deciso di respingere tale reclamo, ritenendo che detta prassi non costituisse una violazione del RGPD.

Disapprovando tale decisione, la Mousse ha adito il Conseil d'État (Consiglio di Stato, Francia) per ottenerne l'annullamento. Il Conseil d'État (Consiglio di Stato) chiede alla Corte di giustizia, in particolare, se la raccolta dei dati relativi all'appellativo dei clienti, limitata ai termini «Signore» e «Signora», possa essere qualificata come lecita e conforme, in particolare, al principio di minimizzazione dei dati, quando tale raccolta sia diretta a consentire una comunicazione commerciale personalizzata nei confronti di tali clienti, conformemente agli usi comunemente ammessi in materia.

La Corte ricorda che, conformemente al principio di minimizzazione dei dati, che costituisce espressione del principio di proporzionalità, i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Inoltre, la Corte ricorda che il RGPD prevede un elenco esaustivo e tassativo dei casi nei quali un trattamento di dati personali può essere considerato lecito: ciò si verifica, in particolare, quando i) è necessario all'esecuzione di un contratto di cui l'interessato è parte, o ii) è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

Per quanto riguarda la prima di queste due giustificazioni, la Corte ricorda che, affinché un trattamento di dati possa essere considerato necessario all'esecuzione di un contratto, tale trattamento deve essere oggettivamente indispensabile al fine di consentire la corretta esecuzione di tale contratto. In tale contesto, la Corte ritiene che una personalizzazione della comunicazione commerciale fondata su un'identità di genere presunta in funzione dell'appellativo del cliente non sembri essere oggettivamente indispensabile per consentire la corretta esecuzione di un contratto di trasporto ferroviario. Infatti, l'impresa ferroviaria potrebbe optare per una comunicazione basata su formule di cortesia generiche, inclusive e prive di correlazione con la presunta identità di genere dei clienti, il che costituirebbe una soluzione praticabile e meno invasiva.

Per quanto riguarda la seconda giustificazione, la Corte, pur richiamando la sua costante giurisprudenza in materia, precisa che il trattamento di dati relativi all'appellativo dei clienti di un'impresa di trasporto, avente la finalità di personalizzare la comunicazione commerciale fondata sulla loro identità di genere, non può essere considerato necessario (i) qualora il legittimo interesse perseguito non sia stato indicato a tali clienti al momento della raccolta di tali dati; (ii) qualora il trattamento non sia effettuato nei limiti dello stretto necessario per la realizzazione di tale legittimo interesse; oppure (iii) qualora, alla luce dell'insieme delle circostanze pertinenti, i diritti e le libertà fondamentali di tali clienti possano prevalere su tale legittimo interesse, in particolare a causa di un rischio di discriminazione fondata sull'identità di genere.

INTELLIGENZA ARTIFICIALE.

7 Gennaio 2025 – I principali trend e sviluppi attesi nel 2025 per l'Intelligenza Artificiale.

Il 2025 è l'anno della prima applicazione pratica di alcune parti del Regolamento UE 2024/1689 sull'Intelligenza Artificiale (AI Act). Ad esempio, a partire dal 2 febbraio 2025 saranno applicabili gli obblighi di alfabetizzazione del personale in materia di IA e potranno essere impiegate nella contrattualistica le definizioni ufficiali dell'articolo 3 dell'AI Act.

Ma il 2025 sarà anche l'anno in cui sono attesi sviluppi ancora più consistenti della capacità dell'IA. Si pensi alla cosiddetta "*Intelligenza Artificiale Agente*", veri e propri agenti AI capaci di agire

autonomamente, prendendo decisioni autonome e ottimizzando processi. Ad esempio: assistenti virtuali non solo in grado di rispondere a domande, ma di gestire intere campagne di marketing, personalizzare l'esperienza utente in tempo reale e automatizzare task complessi. Questo porterà a una nuova era dell'automazione del lavoro e della personalizzazione spinta.

IL 2025 porterà a nuove sfide per la cybersecurity e le aziende dovranno rafforzare le proprie misure di sicurezza per far fronte a minacce completamente nuove, come gli attacchi di tipo *prompt injection*, in cui input dannosi vengono camuffati da messaggi apparentemente legittimi e introdotti nei sistemi di intelligenza artificiale generativa. Anche i progressi nel *quantum computing* metteranno in discussione i metodi tradizionali di crittografia.

Le ricerche pubblicate di recente da Cisco, Gartner e Capgemini Research Institute identificano infine i seguenti 10 trend che caratterizzeranno l'IA nel 2025:

#1: l'AI agenziale ridisegna il futuro dell'automazione del lavoro
#2: la robotica guidata dall'AI sfuma i confini tra uomo e macchina
#3: spazio alle piattaforme di governance per l'IA
#4: nuovi tool per contrastare la disinformazione e proteggere l'integrità dei brand
#5: crittografia post-quantistica per prepararsi alle minacce future
#6: l'era dell'intelligenza ambientale invisibile
#7: il calcolo computazionale ad alta efficienza energetica riduce l'impronta carbonica dell'IT
#8: l'informatica spaziale si diffonde in azienda
#9: i robot polifunzionali migliorano la collaborazione uomo-macchina
#10: il calcolo ibrido per superare i limiti dei modelli analitici attuali.

MERCATI DIGITALI

17 Gennaio 2025 – Il Regolamento DORA sulla resilienza operativa digitale è pianamente applicabile.

Dal 17 gennaio 2025, dopo essere entrato in vigore il 16 gennaio 2023, il Regolamento 2022/2554 - *Digital Operational Resilience Act* (DORA) è pienamente applicabile alle entità finanziarie all'interno dell'UE.

Il Regolamento DORA prescrive requisiti uniformi in materia di sicurezza delle reti e dei sistemi informativi a sostegno delle attività commerci ali delle entità finanziarie, compresi gli enti creditizi, gli istituti di pagamento, le imprese di investimento, i fornitori di critpoattività. Sono indirettamente interessati alla sua applicazione anche i fornitori terzi di servizi TIC.

Il Regolamento DORA ha introdotto diversi requisiti tecnici, organizzativi e documentali per la gestione della resilienza operativa digitale, tra cui:

- la gestione dei rischi relativi alle TIC, comprese le valutazioni dei rischi, le politiche e il monitoraggio delle minacce;
rilevamento e segnalazione di incidenti, tra cui (1) individuare i principali incidenti connessi alle TIC e notificare, su base volontaria, alle autorità competenti le minacce informatiche significative; (2) la segnalazione alle autorità competenti di gravi incidenti operativi o di sicurezza relativi ai pagamenti da parte di determinate entità finanziarie;
- completare una serie di valutazioni, test, metodologie e pratiche per identificare debolezze, carenze e lacune nella resilienza operativa digitale;
- condividere informazioni e intelligence in relazione alle minacce informatiche e alle vulnerabilità; e
- l'attuazione di misure per la corretta gestione dei rischi relativi alle TIC derivanti da terzi, quali l'esecuzione di una valutazione preliminare, l'attuazione di una strategia relativa ai rischi relativi alle TIC da parte di terzi e di un registro di informazioni sugli accordi contrattuali, nonché l'inclusione di disposizioni contrattuali fondamentali negli accordi contrattuali.

---

16 Gennaio 2025 – Consiglio UE: pubblicata in Gazzetta dell'UE la strategia europea in materia di giustizia elettronica 2024-2028.

È stata pubblicata in Gazzetta Ufficiale dell'UE la comunicazione C/2025/437 del Consiglio UE avente ad oggetto la strategia europea in materia di giustizia elettronica 2024-2028.

Essa si applica a tutti gli Stati membri e dovrebbe servire da riferimento per tutti gli attori dell'UE coinvolti nel processo di trasformazione digitale nel settore della giustizia.

La strategia mira a individuare gli obiettivi strategici e operativi e i principi che dovrebbero essere rispettati nello svolgimento di tale processo di trasformazione digitale, mettendo in atto misure organizzative e metodologiche, individuando i fattori chiave per facilitare e promuovere la digitalizzazione, nonché promuovendo meccanismi volti ad agevolare il coordinamento e il follow-up dei progressi compiuti nelle iniziative in materia di giustizia elettronica.

In particolare, la comunicazione detta sia princìpi *sostanziali* che di *funzionamento*.

Tra i primi rientrano il rispetto dei principi e dei diritti fondamentali; l'accesso alla giustizia; la centralità delle persone; colmare il divario digitale; rafforzare le tutele digitali per gli utenti; rendere il sistema sostenibile.

Tra i principi di *funzionamento* la comunicazione menziona il principio «una tantum»; il principio cosiddetto di "*digital by default*"; interoperabilità e cibersicurezza; giustizia dinamica; la giustizia basata sui dati; l'open source.

L'obiettivo generale della giustizia elettronica deve sempre essere quello di migliorare la prestazione dei servizi di giustizia al pubblico al fine di agevolare il godimento del diritto a una tutela giurisdizionale effettiva.

In quest'ottica, dovrebbero essere perseguiti i seguenti obiettivi strategici:

- migliorare l'accesso alla giustizia digitale;
- rafforzare la cooperazione giudiziaria digitale;
- rendere più efficiente la giustizia digitale;
- promuovere una giustizia digitale innovativa.

INFORMATION TECHNOLOGY

10 Gennaio 2025 – In vigore dal 25 Gennaio 2025 le nuove norme per lo svolgimento della mediazione civile e commerciale con modalità telematiche.

Con la pubblicazione sulla Gazzetta Ufficiale del 10 gennaio 2025 n. 7 del decreto legislativo 216/2024 - correttivo della Cartabia e in vigore dal 25 gennaio 2025 - sono state introdotte importanti novità e aggiornamenti al sistema della mediazione civile e commerciale, con l'obiettivo di rendere più efficiente e moderna la mediazione.

Il nuovo articolo 8-*bis* del d.lgs. 28/2010 – rubricato *Mediazione in modalità telematica* – dispone la digitalizzazione del processo di mediazione, con il consenso delle parti. In tal caso, gli atti del procedimento sono formati dal mediatore e sottoscritti con le firme digitali. A conclusione del procedimento il mediatore forma un documento informatico contenente il verbale e l'eventuale accordo per l'apposizione della firma digitale da parte dei soggetti che vi sono tenuti (il documento va immediatamente firmato e restituito al mediatore). Il mediatore, ricevuto il documento e verificata l'apposizione, la validità e l'integrità delle firme, appone la propria firma e ne cura il deposito presso la segreteria dell'organismo, che lo invia alle parti e ai loro avvocati, se nominati.

Il nuovo articolo 8-*ter* del d.lgs. 28/2010 – rubricato *Incontri di mediazione con modalità audiovisive da remoto* – prevede che ciascuna parte può sempre chiedere al responsabile dell'organismo di mediazione di partecipare agli incontri con collegamento audiovisivo da remoto, purché questo assicuri la contestuale, effettiva e reciproca udibilità e visibilità delle persone collegate.