DIGITAL OMNIBUS: PSEUDONIMIZZAZIONE, INTELLIGENZA ARTIFICIALE, DATA BREACH ED E-PRIVACY AL VAGLIO DELL'EDPB E DELL'EDPS

6 marzo 2026

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Partner

Giovanni Lombardi
Associate

Alessandro Carlini
Associate

Il 10 febbraio 2026, l'European Data Protection Board ("**EDPB**") e l'European Data Protection Supervisor ("**EDPS**") hanno pubblicato il Joint Opinion 2/2026 sulla proposta di regolamento nota come "*Digital Omnibus*", con cui la Commissione europea - sulla base della proposta COM(2025) 836 final del 19 novembre 2025 - intende razionalizzare il quadro normativo digitale dell'Unione, intervenendo su un corpus ampio e eterogeneo di atti fondamentali: il Regolamento (UE) 2016/679 ("**GDPR**"), il Regolamento (UE) 2018/1725 ("**EUDPR**"), il Data Act, il Data Governance Act, la direttiva ePrivacy, la Cybersecurity Directive, la direttiva NIS 2, il Single Digital Gateway Regulation e ulteriori strumenti dell'ecosistema digitale europeo. L'obiettivo dichiarato è quello di ridurre gli oneri amministrativi per imprese e pubbliche amministrazioni, migliorare la coerenza tra normative digitali e favorire lo sviluppo dell'economia dei dati, in linea con le più recenti priorità della Commissione in materia di competitività europea.

Nel loro parere, EDPB ed EDPS accolgono con favore alcune misure di semplificazione e armonizzazione, riconoscendo la valenza positiva delle iniziative volte a facilitare la conformità delle organizzazioni al GDPR, rafforzare la certezza giuridica e promuovere l'innovazione responsabile. Il parere congiunto si inserisce nel solco già tracciato dalla *Helsinki Statement on Enhanced Clarity, Support and Engagement* adottata dall'EDPB il 2 luglio 2025, con la quale il Comitato si era impegnato a sviluppare strumenti pratici - tra cui modelli pronti all'uso per le imprese, template comuni per le notifiche di data breach e linee guida accessibili - al fine di ridurre l'onere della conformità, in particolare per le micro, piccole e medie imprese.

Allo stesso tempo, tuttavia, le due autorità esprimono **preoccupazioni significative** su talune modifiche proposte - in particolare con riferimento alla definizione di dato personale e al trattamento dei dati nel contesto dell'intelligenza artificiale - ritenute suscettibili di incidere in modo rilevante sull'attuale livello di tutela garantito dal GDPR. Sono quattro gli ambiti di particolare interesse che emergono dal Joint Opinion 2/2026 e che si analizzeranno nel presente contributo: la disciplina della pseudonimizzazione, il trattamento dei dati nell'ambito dei sistemi di

intelligenza artificiale, le notifiche di data breach e le modifiche al quadro normativo ePrivacy.

PSEUDONIMIZZAZIONE E DEFINIZIONE DI DATO PERSONALE

Uno degli aspetti più controversi della proposta Digital Omnibus riguarda la modifica della definizione di dato personale contenuta nell'articolo 4(1) GDPR. La Commissione propone di introdurre un nuovo paragrafo secondo cui un'informazione non costituisce necessariamente dato personale per ogni soggetto che la tratta, bensì soltanto per quelle entità che dispongono dei mezzi ragionevolmente utilizzabili per identificare l'interessato. Nella prospettiva della Commissione, l'emendamento mirerebbe a "codificare" la giurisprudenza della Corte di Giustizia dell'Unione Europea ("CGUE") sviluppatasi in materia di pseudonimizzazione, con particolare riferimento alla sentenza del 4 settembre 2025 nel caso EDPS c. SRB (C - 413/23 P, ECLI:EU:C:2025:645), nonché alle pronunce precedenti - tra cui la sentenza del 9 novembre 2023 nel caso *Gesamtverband Autoteile - Handel eV c. Scania CV AB* (C - 319/22) - che avevano già delineato un approccio relativo e contestuale alla nozione di dato personale.

Il cuore della modifica proposta risiede nell'ultima frase del nuovo testo, ove si precisa che le informazioni non diventano personali per una determinata entità per il solo fatto che un destinatario successivo possa disporre dei mezzi per identificare l'interessato. Secondo EDPB ed EDPS, questa formulazione - di segno negativo - non rispecchia fedelmente la giurisprudenza della CGUE, la quale ha invece costantemente riaffermato che dati altrimenti non personali possono "diventare" dati personali per l'entità che li mette a disposizione di un destinatario dotato di mezzi ragionevolmente utilizzabili per l'identificazione. La CGUE ha anzi confermato, nella sentenza EDPS c. SRB, che in tali ipotesi i dati sono personali sia per il destinatario sia, indirettamente, per l'entità che li ha trasmessi. La proposta della Commissione trascura dunque un elemento fondamentale della costruzione giurisprudenziale europea.

▼ Il rischio operativo per le organizzazioni

La definizione di dato personale costituisce il perno dell'intero sistema europeo di protezione dei dati, essendo direttamente richiamata dall'articolo 8 della Carta dei Diritti Fondamentali dell'Unione Europea e dall'articolo 16 del TFUE. Un'eventuale restrizione del perimetro applicativo del GDPR - operata per via di modifica legislativa o, ancor più, attraverso atti di esecuzione della Commissione - potrebbe indurre i titolari del trattamento a strutturare artificiosamente le proprie architetture di data governance al fine di escludere determinate attività dall'ambito della disciplina: un rischio concreto, sottolineato con forza nel Joint Opinion 2/2026, paragrafi 16 e 17.

Sul piano pratico, molte architetture di intelligenza artificiale, di analisi avanzata dei dati e di data sharing si fondano su tecniche di pseudonimizzazione. L'incertezza giuridica sulla qualificazione dei dati pseudonimizzati potrebbe tradursi in difficoltà concrete per i compliance officer, i DPO e i consulenti legali chiamati a valutare se e in che misura il GDPR si applichi a specifici trattamenti. L'EDPB è peraltro al lavoro su nuove linee guida in materia di pseudonimizzazione (Guidelines 01/2025, in consultazione pubblica) e di anonimizzazione, che terrà conto anche dell'evoluzione giurisprudenziale.

Un ulteriore profilo critico riguarda la proposta di introdurre un nuovo articolo 41a GDPR, che attribuirebbe alla Commissione il potere di adottare atti di esecuzione per specificare i mezzi e i criteri in base ai quali determinare se i dati risultanti dalla pseudonimizzazione non costituiscano più dati personali per determinate entità. Secondo l'opinione congiunta, tale scelta si presta a una triplice critica: in primo luogo, potrebbe incidere - di fatto - sull'ambito di applicazione materiale del GDPR mediante uno strumento di rango inferiore alla legge, bypassando il procedimento legislativo ordinario; in secondo luogo, affidare alla Commissione stessa la definizione dei criteri per l'applicazione del GDPR appare in contrasto con l'indipendenza delle autorità di controllo garantita dall'articolo 8(3) della Carta; in terzo luogo, la previsione potrebbe generare nuova incertezza interpretativa, anziché ridurla, poiché le conseguenze pratiche degli atti di esecuzione - se essi fondino una presunzione relativa di non-identificabilità o fungano da mero fattore tra altri - restano del tutto indeterminate.

Per tutte queste ragioni, EDPB ed EDPS **invitano con fermezza i co - legislatori a non adottare le modifiche proposte alla definizione di dato personale** e a eliminare il proposto articolo 41a GDPR dalla Proposta, ritenendo che le questioni interpretative sollevate dall'evoluzione giurisprudenziale possano essere meglio affrontate attraverso ulteriori linee guida dell'EDPB, che tengano conto dell'intero corpus giurisprudenziale della CGUE, anziché mediante una modifica legislativa parziale e potenzialmente fuorviante.

INTELLIGENZA ARTIFICIALE E BASI GIURIDICHE DEL TRATTAMENTO

Il Joint Opinion 2/2026 affronta il delicato rapporto tra il GDPR e lo sviluppo di sistemi di intelligenza artificiale, tema che si è imposto nell'agenda regolatoria europea con crescente urgenza a seguito dell'entrata in vigore dell'AI Act (Regolamento (UE) 2024/1689). La proposta Digital Omnibus introduce una disposizione esplicita - il proposto articolo 88c GDPR - secondo cui il trattamento di dati personali nel contesto dello sviluppo e dell'operatività di sistemi o modelli di intelligenza artificiale può fondarsi sul legittimo interesse del titolare del trattamento, quale base giuridica ai sensi dell'articolo 6(1)(f) GDPR.

EDPB ed EDPS osservano, in primo luogo, che il ricorso al legittimo interesse in tale contesto è già possibile sulla base del quadro normativo vigente, come l'EDPB ha già esplicitamente confermato nella propria Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adottata il 17 dicembre 2024. L'introduzione di una disposizione specifica nell'articolato del GDPR non sembra pertanto apportare chiarimenti giuridici di rilievo; al contrario, essa rischia di generare l'impressione che il legittimo interesse costituisca una base giuridica "privilegiata" per i trattamenti connessi all'AI, con conseguente depotenziamento delle garanzie individuali.

Sul piano delle condizioni sostanziali, il parere richiama la necessità che il titolare del trattamento conduca in ogni caso un rigoroso test a tre stadi, codificato nelle EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR: (i) l'esistenza di un interesse legittimo in capo al titolare o a un terzo; (ii) la necessità del trattamento rispetto al perseguimento di tale interesse; (iii) la prevalenza o meno dei diritti e delle libertà fondamentali dell'interessato, quale esito di un bilanciamento caso per caso. Tale valutazione non può essere compressa o generalizzata in ragione della mera appartenenza del trattamento al dominio dell'intelligenza artificiale.

▼ Il diritto all'opposizione nel contesto dell'AI

Il proposto articolo 88c GDPR introduce, al secondo paragrafo, un "diritto all'opposizione incondizionato" come misura di attenuazione del rischio per gli interessati. L'EDPB e l'EDPS accolgono favorevolmente questa misura, ma raccomandano di inserire tale diritto nell'articolo 21 GDPR - piuttosto che in una disposizione autonoma - e di chiarire che esso va portato all'attenzione degli interessati in anticipo, prima dell'inizio del trattamento, tenendo conto delle difficoltà tecniche di rimozione dei dati da sistemi AI già addestrati. L'efficacia del diritto all'opposizione dipende, in ultima analisi, dalla possibilità materiale di far cessare o limitare il trattamento e di eliminare i dati eventualmente già incorporati nei parametri del modello.

Un secondo profilo di grande rilievo pratico riguarda la proposta di introdurre una deroga - attraverso il nuovo articolo 9(2)(k) GDPR - per il trattamento incidentale e residuale di categorie particolari di dati personali durante lo sviluppo e l'addestramento di sistemi o modelli di intelligenza artificiale. L'esigenza che questa deroga intende soddisfare è reale: quando si raccolgono dati per addestrare modelli su larga scala - si pensi ai general - purpose AI models - non è sempre tecnicamente possibile evitare che nel dataset compaiano informazioni relative alla salute, all'orientamento sessuale, alle convinzioni politiche o religiose degli interessati, in quanto tali qualificabili come categorie particolari ai sensi dell'articolo 9 GDPR.

Le autorità riconoscono dunque la legittimità dell'obiettivo perseguito dalla Proposta; tuttavia, propongono una serie di miglioramenti finalizzati a circoscrivere rigorosamente la deroga. In primo luogo, il riferimento al trattamento "incidentale

e residuale" dovrebbe essere espressamente riportato nel testo dispositivo dell'articolo 9(2)(k) GDPR, e non soltanto nel considerando, per evitare interpretazioni estensive che finiscano per coprire anche trattamenti deliberati di dati sensibili. In secondo luogo, il proposto articolo 9(5) GDPR dovrebbe prevedere esplicitamente, quale condizione preliminare di applicabilità della deroga, che la cancellazione dei dati in questione sia impossibile o comporti sforzi sproporzionati, e che tale valutazione sia adeguatamente documentata. In terzo luogo, le garanzie di protezione dovrebbero estendersi all'intero ciclo di vita del sistema AI, ivi inclusa la fase di deployment, al fine di prevenire non solo la raccolta non intenzionale ma anche il riutilizzo dei dati per finalità diverse.

Il parere segnala infine la necessità di coordinare la deroga proposta nell'articolo 9(2)(k) GDPR con il nuovo articolo 4a dell'AI Act - introdotto dalla connessa AI Omnibus Proposal - che prevede un regime distinto per il trattamento di categorie particolari di dati *deliberatamente raccolti* al solo scopo di rilevazione e correzione dei bias. I due regimi non sono sovrapponibili e richiedono una delimitazione normativa chiara per evitare incertezze applicative, specialmente per i fornitori di sistemi AI che operano a cavallo delle due discipline.

DATA BREACH: VERSO UNA MAGGIORE ARMONIZZAZIONE DELLE NOTIFICHE

Tra gli interventi accolti più positivamente dal Joint Opinion 2/2026 figurano le proposte di armonizzazione e semplificazione delle procedure di notifica delle violazioni di dati personali, disciplinate dagli articoli 33 e 34 GDPR. L'analisi dell'EDPB e dell'EDPS si articola su tre piani distinti: la soglia di notifica, la standardizzazione degli strumenti operativi e l'introduzione di un punto di contatto unico (Single Entry Point, "SEP") a livello europeo.

Con riferimento alla soglia di notifica alle autorità di controllo, la Commissione propone di elevare il livello di attivazione dell'obbligo, circoscrivendolo alle violazioni che determinano un rischio elevato per i diritti e le libertà degli interessati, in linea con la soglia già prevista per la notifica agli interessati dall'attuale articolo 34 GDPR. EDPB ed EDPS accolgono favorevolmente tale modifica: da un lato, non si prevede che essa pregiudichi significativamente la protezione degli interessati, stante il persistente obbligo di documentazione interna di qualsiasi violazione ai sensi dell'articolo 33(5) GDPR; dall'altro, essa consentirebbe alle autorità di controllo di concentrare le proprie risorse - già sottoposte a una pressione crescente, come testimoniato dai dati dell'autorità danese che nel 2025 ha ricevuto 9.302 notifiche e di quella irlandese che nel 2024 ne ha gestite 7.781 - sulle violazioni effettivamente ad alto rischio.

Sul fronte dei termini di notifica, la Proposta estende da 72 a 96 ore il termine entro il quale i titolari devono notificare la violazione all'autorità competente. EDPB ed EDPS supportano questa estensione, ritenendo che il termine attuale di 72 ore sia

spesso difficilmente compatibile con i fine settimana e i giorni festivi, in particolare per le organizzazioni più piccole. L'allungamento del termine è atteso migliorare la qualità delle notifiche, consentendo ai titolari di raccogliere informazioni più complete e di adottare misure di rimedio già prima dell'invio. Il parere segnala tuttavia, con preoccupazione, l'esigenza di un maggiore allineamento con le scadenze più brevi previste da altri strumenti normativi europei: NIS 2 impone notifiche entro 24 o 72 ore, DORA entro 24 o 72 ore, eIDAS entro 24 ore e la direttiva CER entro 24 ore. Questa frammentazione rischia di complicare la gestione degli incidenti di sicurezza per le organizzazioni soggette a più regimi normativi.

▼ Il Single - Entry Point e il ruolo dell'EDPB nella standardizzazione

La Proposta prevede l'istituzione di un SEP per la notifica delle violazioni di dati personali, in applicazione dell'articolo 23a della direttiva NIS 2 (2022/2555). Il SEP a livello europeo è accolto con forte favore da EDPB ed EDPS, che lo considerano uno strumento capace di ridurre l'onere amministrativo delle organizzazioni operanti in più Stati membri, senza diminuire il livello di protezione degli interessati. Le autorità sottolineano tuttavia la necessità di garantire la sicurezza delle comunicazioni trasmesse attraverso il SEP, data la sensibilità dei dati contenuti nelle notifiche di violazione.

In parallelo, la Proposta affida all'EDPB la predisposizione di un template comune per le notifiche di data breach e di un elenco di circostanze in cui una violazione è suscettibile di generare un rischio elevato, con la possibilità per la Commissione di modificare tali strumenti attraverso atti di esecuzione. EDPB ed EDPS ritengono questa attribuzione di poteri alla Commissione inappropriata: il template e l'elenco delle circostanze dovrebbero essere preparati e approvati esclusivamente dall'EDPB, in modo analogo al potere di approvazione dei criteri di certificazione già riconosciuto dall'articolo 42(5) GDPR, al fine di garantire indipendenza e coerenza nell'interpretazione della norma.

Nella medesima prospettiva di armonizzazione, la Proposta introduce la creazione di liste comuni EEA di attività di trattamento per le quali è obbligatoria o non obbligatoria la valutazione d'impatto sulla protezione dei dati ("DPIA"), nonché di un template e di una metodologia comuni per la conduzione delle DPIA stesse. EDPB ed EDPS accolgono favorevolmente queste iniziative, che - in linea con la Dichiarazione di Helsinki - contribuiranno a ridurre la frammentazione tra autorità nazionali e ad alleggerire il carico di conformità per le imprese. Si raccomanda tuttavia che la nozione di "metodologia" per la DPIA sia intesa in senso ampio e pratico - come processo strutturato e principi applicativi, e non come mera checklist - al fine di preservare la necessaria flessibilità in ragione della varietà dei contesti di trattamento.

E-PRIVACY E COOKIE: VERSO UN SUPERAMENTO DELLA *CONSENT FATIGUE*?

Il Joint Opinion 2/2026 affronta, infine, le modifiche rilevanti alla direttiva ePrivacy (2002/58/CE), con particolare riferimento alla protezione delle informazioni memorizzate nei terminali degli utenti - i cosiddetti cookie e tecnologie analoghe. Si tratta di un ambito in cui la necessità di riforma è largamente riconosciuta: la proliferazione di banner cookie e richieste di consenso non ha, nella pratica, rafforzato la consapevolezza degli utenti, ma ha semmai alimentato il fenomeno della "consent fatigue", con effetti paradossalmente regressivi sulla qualità del consenso prestato.

La proposta Digital Omnibus interviene su questo terreno con un approccio duplice: da un lato, introduce nuove disposizioni - il proposto articolo 88a GDPR - che stabiliscono eccezioni all'obbligo di consenso per l'accesso e la memorizzazione di informazioni nei terminali degli utenti; dall'altro, prevede meccanismi automatizzati e leggibili dalle macchine per l'espressione delle preferenze degli utenti - il proposto articolo 88b GDPR. EDPB ed EDPS sostengono con forza l'obiettivo sotteso a entrambe le disposizioni: semplificare la gestione del consenso, ridurre l'onere sia per gli utenti sia per i titolari del trattamento e promuovere scelte più reali e consapevoli.

Le eccezioni al consenso previste dal proposto articolo 88a(3) GDPR riguardano, in particolare: (i) la fornitura di un servizio esplicitamente richiesto dall'utente; (ii) la misurazione dell'audience di un servizio online da parte del suo gestore, per uso esclusivamente interno; (iii) la sicurezza del servizio o del terminale. Rispetto all'attuale articolo 5(3) della direttiva ePrivacy, la Proposta introduce un'eccezione più ampia per la fornitura del servizio richiesto - non limitata ai servizi della società dell'informazione - e aggiunge le nuove eccezioni per la misurazione dell'audience e la sicurezza. EDPB ed EDPS raccomandano di circoscrivere rigorosamente ciascuna eccezione a quanto strettamente necessario: in particolare, la misurazione dell'audience dovrebbe essere limitata a informazioni aggregate anonime, non utilizzabili per finalità ulteriori e non combinate con dati provenienti da altri servizi o terzi.

Un ulteriore aspetto di rilievo riguarda la proposta di introdurre una specifica eccezione per la pubblicità contestuale, ossia la pubblicità basata sul contesto di navigazione attuale dell'utente, priva di tracciamento inter - siti e di memorizzazione a lungo termine. EDPB ed EDPS ritengono che tale forma pubblicitaria, meno invasiva rispetto alla pubblicità comportamentale, possa essere inserita nell'elenco delle eccezioni al consenso, a condizione che l'eccezione sia chiaramente delimitata e non si presti ad usi abusivi che ne amplino di fatto la portata. La proposta, ove ben circoscritta, potrebbe costituire un incentivo

economico alla diffusione di modelli pubblicitari rispettosi della privacy, riducendo la pressione verso il tracciamento invasivo.

Sul tema del rinnovo del consenso, il proposto articolo 88a(4) GDPR introduce salvaguardie specifiche: in particolare, il titolare non potrà formulare una nuova richiesta di consenso per sei mesi in caso di rifiuto dell'utente. EDPB ed EDPS accolgono positivamente queste cautele, raccomandando al contempo la definizione di un periodo massimo di validità del consenso originariamente prestato, al fine di garantire che gli utenti siano periodicamente rimessi nella condizione di rivedere le proprie scelte. Si suggerisce, infine, di prevedere un'eccezione esplicita al consenso per la registrazione del rifiuto stesso, necessaria tecnicamente per l'attuazione del divieto di reiterazione delle richieste, a condizione che tale eccezione si traduca nell'utilizzo di un identificatore generico e anonimo, comune a tutti gli utenti che abbiano rifiutato il consenso.

Il parere congiunto evidenzia, infine, un profilo trasversale di primaria importanza: le nuove disposizioni ePrivacy non potranno essere effettivamente attuate e sanzionate senza un adeguato potenziamento dei poteri correttivi delle autorità di protezione dei dati. I proposti articoli 88a e 88b GDPR devono essere accompagnati da espliciti riferimenti alle disposizioni sanzionatorie degli articoli 83(5) GDPR e 66(3) EUDPR, al fine di garantire *una effettiva deterrenza* nei confronti dei soggetti non conformi.

EQUILIBRIO DIFFICILE TRA SEMPLIFICAZIONE E PROTEZIONE

Il Joint Opinion 2/2026 di EDPB ed EDPS sul Digital Omnibus riflette con chiarezza la complessità e la delicatezza della fase che il diritto digitale europeo sta attraversando. La proposta della Commissione si muove su un doppio binario: da un lato, misure di semplificazione genuine e auspicabili - come l'armonizzazione delle notifiche di data breach, la standardizzazione delle DPIA, il contrasto alla consent fatigue - che gli stessi EDPB ed EDPS accolgono con favore; dall'altro, modifiche strutturali alla definizione di dato personale e al regime delle basi giuridiche per l'AI che le autorità considerano inopportune, premature o addirittura controproducenti rispetto agli obiettivi dichiarati.

Sul fronte della pseudonimizzazione, la scelta di intervenire per via legislativa su una definizione che la CGUE ha progressivamente elaborato attraverso una giurisprudenza raffinata e contestuale desta le preoccupazioni più acute. L'eventuale adozione del proposto articolo 4(1) GDPR nella versione presentata dalla Commissione - e, ancor più, del proposto articolo 41a GDPR - potrebbe inaugurare una stagione di elusione sistematica del GDPR, attraverso architetture di trattamento studiate ad arte per sottrarre determinati flussi di dati all'applicazione della normativa. Il rimedio indicato nel parere - ulteriori linee guida dell'EDPB, anziché intervento legislativo - appare più idoneo a garantire

un'evoluzione ordinata del quadro giuridico, nel rispetto delle competenze istituzionali delle autorità di controllo.

Sul fronte dell'intelligenza artificiale, la sfida normativa è di diversa natura: non si tratta di correggere un intervento potenzialmente lesivo, ma di assicurare che le disposizioni introdotte - legittimo interesse per l'AI, deroga per il trattamento incidentale di categorie speciali - siano accompagnate da garanzie sufficientemente robuste e da criteri applicativi chiari. Il coordinamento con l'AI Act rimane un cantiere aperto, che richiederà un'attenta opera di raccordo normativo nei prossimi mesi, anche alla luce dell'entrata in applicazione progressiva dei diversi obblighi previsti dal Regolamento.

In ultima analisi, il processo legislativo che seguirà nei prossimi mesi - con il coinvolgimento del Parlamento europeo e del Consiglio - sarà decisivo per determinare se la revisione del digital rulebook europeo saprà trovare il punto di equilibrio tra semplificazione normativa, stimolo all'innovazione e tutela effettiva dei diritti fondamentali degli individui. Il parere congiunto delle due principali autorità europee di protezione dei dati rappresenta, in questo contesto, un contributo di straordinario valore: non solo per la profondità dell'analisi tecnico - giuridica, ma anche per la chiarezza con cui vengono tracciate le linee di confine oltre le quali la semplificazione rischia di diventare regressione.

AUTORI

Aurora Agostini

Partner

Giulietta Minucci

Partner

Giovanni Lombardi

Associate

Alessandro Carlini

Associate