

Omniter Group SRL michele.scarabello@omniter.it Tel. 0498842717 Cell. 3939702687		Omniter Consulenze Aziendali	Sicurezza D.lgs 81/08 C.P.R. CE B.R.C. ISO 22716 Qualità ISO 14001 UL OHSAS 18001 Reg.1223 Rumore Vibrazioni Ambiente D.lgs. 231/01 ISO 9001 B.C.M. Formazione I.F.S.	NEWS 12/2025 Pagina 1 di 1 RISERVATO
1	SLITTA APPLICAZIONE EUDR			
Slitta a dicembre 2026	Il 26 novembre 2025, Il Parlamento europeo ha approvato una serie di modifiche al regolamento europeo contro la deforestazione (EUDR), la normativa che assicura che i prodotti immessi nel mercato dell'UE non provengano da terreni deforestati. Le modifiche mirano a facilitare l'applicazione da parte delle imprese e dei partner commerciali, offrendo una transizione più graduale. Cosa prevede la proposta approvata Prevede il rinvio di 12 mesi per l'entrata in vigore delle norme per tutte le imprese: Grandi aziende: da 30 dicembre 2026 Micro e piccole imprese: dal 30 giugno 2027 Il rinvio consentirà di potenziare il sistema informatico europeo per le dichiarazioni elettroniche di due diligence. Modifiche ai requisiti di due diligence 1. Obblighi mirati per le imprese Secondo la posizione del Parlamento, la dichiarazione di due diligence dovrà essere presentata da chi immette per primo il prodotto nel mercato dell'UE, semplificando gli obblighi per operatori e commercianti che effettuano solo passaggi successivi. 2. Semplificazioni per micro e piccoli operatori Le micro e piccole imprese primarie dovranno presentare una dichiarazione semplificata e una tantum, riducendo in modo significativo l'onere amministrativo.			
2	USO IA – AGGIORNARE Sistema Gestione Privacy			
Intelligenza Artificiale (IA) uso corretto nel rispetto della privacy	L'intelligenza artificiale (IA) presenta rischi per la privacy, come la raccolta massiva di dati sensibili, la profilazione dettagliata e il rischio di decisioni automatizzate discriminatorie, che violano le normative come il GDPR. Allo stesso tempo, l'IA può contribuire a proteggere i dati attraverso la crittografia e il controllo degli accessi. Normative come il GDPR e l'AI Act in Europa regolano l'uso dell'IA per tutelare la privacy, richiedendo trasparenza, valutazioni del rischio e il diritto all'intervento umano nelle decisioni automatizzate. I sistemi attuati nelle imprese devono essere integrati e definiti nel registro dei trattamenti con adeguata informativa al personale.			
3	VOUCHER A SOSTEGNO DELLA CYBERSICUREZZA			
Previsti aiuto per i progetti 2026	Il Voucher Cloud e Cybersecurity è il nuovo bando nazionale promosso dal Ministero delle Imprese e del Made in Italy (MIMIT) per supportare la trasformazione digitale sicura del tessuto produttivo italiano. L'obiettivo è rafforzare la competitività e la solidità della transizione digitale, colmando il divario tra piccole realtà e grandi organizzazioni L'operatività e la presentazione delle domande sono subordinate al Decreto Attuativo, previsto per l'inizio 2026. Il bando prevede un contributo a fondo perduto fino al 50% - Massimale del contributo: Fino a 20.000 euro per progetto. - Investimento minimo: L'investimento minimo richiesto per accedere all'incentivo è di 4.000 euro. Attenzione: Sono ammissibili solo le spese legate a servizi nuovi o aggiuntivi rispetto a quelli già in uso, o a miglioramenti significativi delle soluzioni esistenti. Le spese ammissibili includono: - Soluzioni hardware e software per la cybersecurity, destinate a proteggere infrastrutture, reti e dati aziendali. - Servizi cloud infrastrutturali (IaaS), utili per l'archiviazione e la gestione scalabile dei dati. - Servizi cloud applicativi (SaaS), come piattaforme gestionali, strumenti collaborativi o CRM. - Servizi di configurazione, monitoraggio e supporto continuativo, essenziali per garantire stabilità e sicurezza nel tempo Le soluzioni acquistate devono essere fornite da soggetti che risultino accreditati presso l'Agenzia per la Cybersecurity Nazionale (ACN) e qualificati come servizi cloud di livello 1 (QC1). Questo requisito garantisce elevati standard di qualità e sicurezza, attestando il rispetto di parametri tecnici e organizzativi precisi (come la protezione dei dati e la gestione dei rischi).			
4	BADGE DIGITALE PER ACCEDERE NEI CANTIERI			
Da gennaio 2026	Il Badge di Cantiere Elettronico è un tesserino digitale con codice anticontraffazione QR o RFID collegato alla Banca Dati Nazionale INL. Contiene dati anagrafici, foto, certificato sanitario e formazione sicurezza. Lo emette il datore di lavoro ed è obbligatorio dal 31 dicembre 2025 per i cantieri pubblici, dal 1° marzo 2026 per i cantieri privati. Le imprese saranno responsabili dell'iscrizione dei propri lavoratori nella piattaforma e del rilascio del badge aggiornato, mentre i committenti dovranno verificare che chiunque acceda all'area di lavoro sia in regola. La mancata osservanza delle nuove prescrizioni può comportare sanzioni significative, calcolate in proporzione al valore dell'appalto, fino alla sospensione dei lavori nei casi più gravi. Nessun addetto privo di badge potrà varcare i cancelli del cantiere. I decreti attuativi, attesi nei prossimi giorni, definiranno le modalità operative precise di emissione e utilizzo del badge - Gli standard tecnici per i codici anticontraffazione - Le procedure di verifica e controllo in cantiere - Le sanzioni specifiche per inadempienza Le imprese edili dovranno prepararsi per tempo, considerando che la transizione verso un cantiere completamente digitale richiede non solo nuovi strumenti tecnologici, ma anche un cambio di mentalità organizzativa.			
5	LINEE GUIDA RUOLO ODV MOG 231/01			
Guida operativa per gli ODV ed il loro ruolo	Il 24 Novembre è stata comunicata ufficialmente la pubblicazione delle "Linee Guida per lo svolgimento delle funzioni dell'Organismo di vigilanza ex D.lgs. 231/2001", elaborato dall'Osservatorio Nazionale sul D.lgs. 231/2001 istituito dal CNDCEC nell'ambito dell'area di delega "Compliance e modelli organizzativi delle imprese". Il Documento nasce con l'obiettivo di fornire un riferimento aggiornato, chiaro e operativo per l'esercizio delle funzioni dell'Organismo di vigilanza, alla luce dell'evoluzione normativa, giurisprudenziale e organizzativa che negli ultimi anni ha reso il ruolo dell'OdV sempre più centrale nei sistemi di controllo interno delle imprese. Le Linee Guida affrontano tematiche centrali per l'effettività dei Modelli di organizzazione, gestione e controllo, dedicando una particolare attenzione alle modalità operative delle verifiche e alla corretta gestione documentale. L'intento è quello di offrire un quadro organico e coerente che possa supportare i professionisti nell'adozione di prassi omogenee e nella gestione delle principali questioni operative che emergono nello svolgimento dell'incarico, contribuendo a rafforzare qualità, affidabilità e riconoscibilità del ruolo degli ODV.			
I nostri tecnici possono darVi assistenza sui punti sopra riportati e sui temi D. LGS 231/01 - PRIVACY - RSPP - ISO9001 - ISO14001 - ISO45001 - BRC - IFS - IATF - PERCORSI FORMATIVI - MARCATURA CE - CONTRIBUTI				
GRADIREI ULTERIORI CHIARIMENTI SUI PUNTI: _____ PER INFORMAZIONI PIÙ DETTAGLIATE (barrare la casella di interesse) E INVIARE PER FAX o E-MAIL DITTA: _____ REFERENTE: _____ TEL: _____ E-MAIL: _____				
Trattamento dei dati e Privacy. In riferimento al trattamento dei dati secondo la legislazione vigente, in particolare Reg. UE 679/16 e D.Lgs. 196/03, si precisa che i dati riportati nel presente documento saranno trattati esclusivamente per i servizi richiesti dal cliente e dagli interessati con i quali viene in contatto (come indicato nell'informativa al punto 2A). L'interessato può esercitare i diritti di cui agli artt.15-22 del Reg. UE 679/16 comunicando con i riferimenti riportati nella informativa che è disponibile sul sito aziendale. La persona che ci comunica i dati di altri interessati, dichiara di essere autorizzata per tali comunicazioni. Clicca per indicare di NON inviare più la Vostra newsletter.				