Studio Violi S.r.l.
Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015

2003-2023

ISO 9001 BUREAU VERITAS Certification IT309277

I Partners dello Studio

Giorgio Violi	tel: 3386132605	givioli@gmail.com
Alberto Sant'Unione	tel: 3409125853	santunionea@gmail.com

Qualità Sicurezza Privacy Ambiente Risk Management
Responsabilità Amministrativa 231 Etica Consulenza e Audit per la Direzione

Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015 per Progettazione ed erogazione di servizi di consulenza relativa ai Sistemi di Gestione Aziendale per la Qualità, la Sicurezza negli ambienti di lavoro, la Privacy, l'Ambiente, l'Etica, per i Modelli Organizzativi e Consulenza per la Direzione

2024 Aprile **Il nostro punto di vista su…** *Anno 17 – 1° sem*

Periodico di informazione per i CLIENTI dello STUDIO VIOLI

Indice delle NOTIZIE (N)

- N1) Privacy: Confindustria, Ania, Abi e Confcommercio: no alla cancellazione dopo 7 giorni dei metadati delle email aziendali

- N2) Privacy: La formazione e l'istruzione degli addetti che trattano dati personali non possono essere uguali per tutti

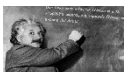
- N3) Privacy: No del Garante Privacy al riconoscimento facciale per controllo presenze dei lavoratori; Regolamento sull'Intelligenza Artificiale, l'utente deve sempre sapere se sta interagendo con un robot; Il metodo 'dai il consenso o paga' viola la privacy degli utenti

- N4) Sicurezza: La formazione obbligatoria e l'aggiornamento del preposto: nuova periodicità biennale dal 21/12/2023

- N5) Sicurezza: Il decreto-legge 19/2024 e le novità della patente a crediti per i cantieri temporanei

SENTENZE DI CASSAZIONE SUL LAVORO

- Sul sito http://www.dottrinalavoro.it/argomento/giurisprudenza-c/corte-di-cassazione-c sono presenti le ultime sentenze di Cassazione relative al lavoro



AFORISMA DEL MESE

"Pianificare è decidere in anticipo cosa fare, come farlo, quando farlo e chi deve farlo. La pianificazione è alla base dell'efficacia"

Winston Churchill (Politico britannico)

Scadenziario di Aprile 2024 sul sito del Sole 24 Ore http://www.ilsole24ore.com/norme-e-tributi/scadenze.shtml

“Prova di resistenza”

Notizie

- N1) Privacy: Confindustria, Ania, Abi e Confcommercio: no alla cancellazione dopo 7 giorni dei metadati delle email aziendali

I metadati delle e-mail aziendali sono uno strumento di lavoro e anche dopo 7 giorni dalla creazione del messaggio la loro natura non cambia.

Non si può perciò imporre al datore di lavoro di scegliere tra cancellarli dopo 7 giorni oppure, se vuole tenerli per più tempo, di fare una trattativa sindacale o di farsi autorizzare dall'ispettorato del lavoro. Al contrario ogni azienda deve poter stabilire in autonomia la regola più appropriata per la conservazione di e-mail e metadati. **È questa la posizione di Confindustria, Ania, Abi e Confcommercio, che hanno inviato al Garante della privacy una nota congiunta, molto critica, per partecipare alla consultazione pubblica sui metadati lanciata dallo stesso Garante (provvedimento n. 127 del 22/2/2024).**

I metadati sono informazioni riferite alle e-mail come, ad esempio, dimensione, giorno, ora, mittente, destinatario e oggetto. Negli atti del Garante (documento di indirizzo adottato con il provvedimento n. 642 del 21/12/2023) si legge che, decorsi 7 giorni (estendibili di 48 ore), conservare i metadati significa controllare i lavoratori e, quindi, bisogna rispettare l'articolo 4, comma 1, della legge 300/1970: i datori di lavoro devono fare l'accordo con i sindacati o, in alternativa, avere l'autorizzazione dell'Ispettorato del lavoro.

L'orientamento del Garante, che risale almeno al 2016 (ingiunzione n. 303 del 13/7/2016) ed è stato applicato molte volte (ad esempio ingiunzione n. 409 dell'1/12/2022), ha suscitato le reazioni critiche delle imprese. **Secondo le associazioni di queste ultime, i metadati sono parte costitutiva delle e-mail e, come queste ultime, sono uno strumento di lavoro, per il quale, ai sensi dell'articolo 4, comma 2, della legge 300/1970, non si applica il procedimento contrattuale/autorizzativo previsto per gli impianti di controllo indiretto a distanza sui lavoratori. Inoltre, la scadenza dei 7 giorni, secondo le imprese, fa saltare la sicurezza: per scoprire incidenti informatici occorre poter fare ricerche sui metadati anche dopo 7 giorni (magari il malware è giacente da mesi negli account).**

La conclusione delle imprese è che non può essere fissato un termine breve e uguale per tutti per la conservazione dei metadati delle e-mail: al contrario, **ogni datore di lavoro deve poterlo definire in base a esigenze gestionali e a obblighi normativi, illustrando le sue scelte nelle policy e nei regolamenti interni sull'uso della e-mail aziendale e nelle informative ai dipendenti** (articolo 4, comma 3, della legge 300/1970).

In materia, peraltro, va sottolineata una possibile mediazione tra le diverse esigenze è distinguere i metadati embedded (inclusi) nei messaggi dai separati file dei log (documenti elettronici diversi e separati contenenti i metadati dei messaggi) e applicare a questi ultimi le prescrizioni di maggiore cautela.

- N2) Privacy: La formazione e l'istruzione degli addetti che trattano dati personali non possono essere uguali per tutti

Nel corso degli ultimi mesi, l'intensificazione dei controlli relativamente alle buone e corrette policy aziendali in materia di privacy, ha, purtroppo, scoperto un nervo ancora troppo dolente;

infatti sempre troppo spesso l'azienda sensibilizzata sì alla creazione di una policy aziendale, dopo aver formalizzato un discreto apparato teorico, nel divenire delle problematiche giornaliere del lavoro, abbandona le procedure operative creando, così, un terreno scivoloso e propenso a qualsiasi "incidente" sulla gestione dei dati.

Il fulcro troppo spesso poco considerato è l'importanza di talune indicazioni dei combinati disposti degli artt. 29 GDPR "chiunque abbia accesso a dati personali", art. 32 "chiunque agisca sotto la loro autorità e abbia accesso a dati personali", art 39 "formazione del personale che partecipa ai trattamenti", art. 2-quaterdecies, Dlgs 196/2003 come modificato dal Dlgs 101/2018 "attribuiti a persone fisiche, espressamente designate".

Di cosa, dunque, stiamo parlando? Di coloro che, istruiti dal titolare del trattamento dati o dal responsabile del trattamento dati se designato, agisco attivamente e trattano i dati personali e non per le finalità espresse dal titolare del trattamento.

Tale ultima enunciazione potrebbe, ai più, sembrare essere un modus operandi che non necessita di particolari abilità; purtroppo, invece, **tali operazioni, oltre ad essere "attività pericolose" così come l'art. 2050 del codice civile riteneva, sempre e comunque con l'ausilio del mai abbastanza compianto Dlgs 196/2003, far rientrare il trattamento dei dati, sono declinabili come abilità che devono avere tutti i soggetti altamente qualificati.**

Vediamo ora dunque quali possono essere definibili le attività propedeutiche da attuare per l'istruzione degli ex incaricati al trattamento dei dati; indirettamente intuiamo l'adempimento dell'istruzione nell'art. 25 del Regolamento (UE) 2016/679 in quanto, se è vero che la progettazione per la protezione dei dati deve essere l'input del Titolare, è anche vero che la prosecuzione delle modalità operative dovranno essere portate a conoscenza dei soggetti a lui gerarchicamente sottoposti.

Tralasciando l'analisi dell'art. 29 che risulta essere ridonante nella comparazione con l'art. 32 del Regolamento (UE) 2016/679, ci soffermeremo ora su quest'ultimo in quanto definibile il cuore dell'adempimento in trattazione. Infatti, il solo titolo dell'articolo definisce l'importanza del suo contenuto: sicurezza del trattamento.

Il punto 4 risulta il vero monito nei confronti dei responsabili - non di nome ma di fatto - che si pronuncia in tal senso "Il Titolare del trattamento e il Responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

Sebbene sia chiaro l'intento del legislatore nel far percepire che chiunque tratti i dati per conto del Titolare del trattamento, a seguito di procedura autorizzativa di accesso alle singole banche dati, non possa procedere in tal senso se non precedentemente istruito, dovremmo tener da conto che, per coloro che avevano ottenuto una formazione anteriormente all'entrata in vigore del Regolamento (UE) 2016/679, possa essere previsto un refresh degli adempimenti da effettuare; per i soggetti, invece, in ingresso alla data di entrata in vigore del Regolamento UE 2016/679 potrebbe dover significare una formazione ex novo con i parametri di seguito definiti. Sarebbe, dunque, possibile riscontrare una differenza di formazione e/o istruzione in base alla data di assunzione di personale dipendente che ha la funzione di trattare i medesimi dati? Sarà, quindi, obbligatorio procedere a un allineamento teorico pratico per tutti i soggetti preposti al trattamento dei dati?

Probabilmente, tabula rasa delle informazioni acquisite precedentemente da un ex incaricato del Trattamento dati potrebbe essere la giusta e corretta operazione al fine di ordinare le operazioni di trattamento da effettuare sui dati personali.

-N3) Privacy: No del Garante Privacy al riconoscimento facciale per controllo presenze dei lavoratori; Regolamento sull'Intelligenza Artificiale, l'utente deve sempre sapere se sta interagendo con un robot;

No del Garante Privacy al riconoscimento facciale per controllo presenze dei lavoratori. Il riconoscimento facciale per controllare le presenze sul posto di lavoro viola la privacy dei dipendenti. Non esiste al momento alcuna norma che consenta l'uso di dati biometrici, come prevede il Regolamento, per svolgere una tale attività. Per questo motivo il Garante privacy ha sanzionato cinque società - impegnate a vario titolo presso lo stesso sito di smaltimento dei rifiuti - con sanzioni rispettivamente di 70mila, 20mila, 6mila, 5mila e 2mila euro, per aver trattato in modo illecito i dati biometrici di un numero elevato di lavoratori. [Vedasi provvedimenti doc. web n. 9995680, 9995701, 9995741, 9995762, 9995785]
L'Autorità, intervenuta a seguito dei reclami di diversi dipendenti, ha anche evidenziato i particolari rischi per i diritti dei lavoratori connessi all'uso dei sistemi di riconoscimento facciale, alla luce delle norme e delle garanzie previste sia nell'ordinamento nazionale che in quello europeo.
Dall'attività ispettiva del Garante, svolta in collaborazione con il Nucleo speciale privacy e frodi tecnologiche della Guardia di finanza, sono emerse anche ulteriori violazioni da parte delle società. In particolare l'Autorità ha accertato che tre aziende avevano condiviso per più di un anno lo stesso sistema di rilevazione biometrica, oltretutto senza aver adottato misure tecniche e di sicurezza adeguate. Inoltre il medesimo "sistema", ritenuto illecito dall'Autorità, era utilizzato presso altre nove sedi dove operava una delle società sanzionate. Le aziende, infine, non avevano fornito una informativa chiara e dettagliata ai lavoratori né avevano effettuato la valutazione d'impatto prevista dalla normativa privacy.
Le aziende, ad avviso del Garante, avrebbero dovuto più opportunamente utilizzare sistemi meno invasivi per controllare la presenza dei propri dipendenti e collaboratori sul luogo di lavoro (come ad es. il badge). Oltre al pagamento delle sanzioni il Garante ha ordinato la cancellazione dei dati raccolti illecitamente.

Regolamento sull'Intelligenza Artificiale, l'utente deve sempre sapere se sta interagendo con un robot. Intelligenza artificiale (IA) mai in incognito. Le persone devono sapere se parlano con un robot o se stanno leggendo un testo prodotto da un'IA. È uno degli strumenti di tutela previsti dal regolamento Ue sull'intelligenza artificiale, approvato dal parlamento Ue il 13 marzo 2024, che disciplina modalità di immissione e di utilizzo nell'area Ue di questi strumenti di elevata tecnologia. Il provvedimento deve passare ancora l'ultimo vaglio del Consiglio Ue, prima di essere pubblicato sulla Gazzetta Ufficiale Ue.
Il regolamento, oltre alla esplicita messa al bando dei sistemi che violano i diritti fondamentali, prevede una fitta serie di regole, parametrate a diversi livelli di rischio (minimo, alto, sistemico), per avere sotto controllo il mercato dell'IA: le autorità devono sapere chi mette in circolazione apparati di IA e, per quelli ad alto rischio, vengono imposti standard di conformità (con apposita marcatura) sotto la vigilanza di autorità pubbliche.
Completano il quadro le disposizioni sulle garanzie per le persone fisiche: devono essere in grado di individuare ciò che proviene da un robot, poter chiedere spiegazioni e informazioni quando si è soggetti a un'IA, ma soprattutto fruiscono di prerogative contro le autorità pubbliche, che usano l'IA per ragioni di contrasto alla criminalità e per la sicurezza.
Un aspetto di primaria importanza nel regolamento è la trasparenza per gli umani. Le persone devono essere informate e consapevoli che stanno dialogando e interagendo con un sistema di IA, salvo che ciò sia già evidente per un soggetto ragionevolmente attento.
I fornitori dei sistemi di IA devono comunque progettare e sviluppare i sistemi in maniera che non sorgano equivoci.
Grava, sempre a carico dei fornitori di sistemi di IA, che generano contenuti audio, immagini, video o testuali sintetici, l'obbligo di garantire che ciò che è prodotto dall'IA sia marcato in un formato leggibile meccanicamente e rilevabile come generato o manipolato artificialmente.
L'obbligo di trasparenza è prescritto anche per gli operatori che utilizzano sistemi di IA di riconoscimento delle emozioni, sistemi di categorizzazione biometrica e sistemi di IA che generano o manipolano immagini o contenuti audio o video, che costituiscono un "deep fake". L'obbligo informativo non scatta, però, in alcuni casi: se si usano i sistemi per ragioni di giustizia penale o, nell'ambito editoriale, se c'è la revisione umana del testo scritto dall'IA e se c'è un responsabile della pubblicazione del contenuto.
Peraltro, i sistemi di IA non saranno considerati ad alto rischio se non presentano un rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali. Non sfuggono mai alla qualifica di alto rischio, invece, se effettuano la profilazione delle persone.
Se un sistema di IA comporta il trattamento di dati personali, deve essere dichiarata la conformità alle norme sulla privacy.
In alcuni casi dovrà essere stilata una valutazione d'impatto sui diritti fondamentali.

Prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio, di norma, il fornitore deve registrarsi in una banca dati dell'Ue.
Dopo l'immissione sul mercato di tali sistemi di IA, i fornitori devono assicurare il monitoraggio post-commercializzazione e, se necessario, adottare misure correttive.
Se si tratta di IA con finalità generali e che presentano un rischio sistemico devono essere rispettati obblighi rafforzati in materia di analisi dei rischi e di valutazione di impatto.

Il metodo 'dai il consenso o paga' viola la privacy degli utenti. Con l'escamotage "Dai il consenso o paga" le grandi piattaforme come Facebook e Instagram violano il GDPR. Questa è la conclusione a cui sono giunte le autorità per la protezione dei dati europee. Nel corso della plenaria del 17 aprile 2024, l'European Data Protection Board ha infatti adottato un parere ai sensi dell'art. 64 (2) del GDPR a seguito delle richieste che gli erano state sottoposte dalle autorità olandese, norvegese e di Amburgo, anche alla luce della sentenza C-252/21 della Corte di Giustizia UE. Il parere del board europeo affronta la validità del consenso al trattamento dei dati personali ai fini della pubblicità comportamentale nel contesto del metodo conosciuto come "Pay or Okay" che le grandi piattaforme online hanno adottato negli ultimi tempi. Per quanto riguarda i modelli "Dai il consenso o paga" implementati dalle grandi piattaforme online, i garanti europei ritengono che, nella maggior parte dei casi, non sarà possibile per loro soddisfare i requisiti per un consenso valido se mettono gli utenti di fronte solo alla scelta tra il consenso trattamento dei dati personali per finalità di pubblicità comportamentale e pagamento di un compenso.
L'EDPB ritiene che offrire solo un'alternativa a pagamento ai servizi che comportano il trattamento di dati personali a fini di pubblicità comportamentale non dovrebbe essere la soluzione predefinita per i titolari del trattamento.
Nello sviluppare alternative, le grandi piattaforme online dovrebbero pertanto prendere in considerazione la possibilità di fornire ai singoli individui un'alternativa equivalente che non comporti il pagamento di una commissione.
Se i titolari del trattamento scelgono di addebitare una tariffa per l'accesso all'alternativa equivalente, dovrebbero prendere in seria considerazione l'offerta di un'alternativa aggiuntiva. Questa alternativa gratuita dovrebbe essere priva di pubblicità comportamentale (per esempio una forma di pubblicità che comporti il trattamento di pochi o nessun dato personale). Questo è un fattore particolarmente importante nella valutazione del consenso valido ai sensi del GDPR.
L'EDPB, che ha preannunciato anche nuove linee guida sul tema, sottolinea che l'ottenimento del consenso non esenta il titolare dal rispetto di tutti i principi delineati nell'art. 5 del GDPR, quali limitazione delle finalità, minimizzazione dei dati e correttezza. Inoltre, le grandi piattaforme online dovrebbero anche considerare il rispetto dei principi di necessità e proporzionalità, e hanno la responsabilità di dimostrare che il loro trattamento è generalmente in linea con il GDPR.
Per quanto riguarda la necessità che il consenso sia libero, dovrebbero essere sempre presi in considerazione i criteri di condizionalità, pregiudizio, squilibrio di potere e granularità. Ad esempio, il board dei garanti sottolinea che qualsiasi tariffa addebitata non può far sentire gli individui obbligati a dare il proprio consenso.
Le autorità dovrebbero valutare, caso per caso, sia se una tariffa sia adeguata sia quale importo sia appropriato nelle circostanze date. Le grandi piattaforme online dovrebbero anche considerare se la decisione di non prestare il consenso può portare l'individuo a subire conseguenze negative, come l'esclusione da un servizio importante, la mancanza di accesso a reti professionali o il rischio di perdere contenuti o connessioni.
L'European Data Protection Board rileva che è probabile che si verifichino conseguenze negative quando le grandi piattaforme online utilizzano un modello "consenso o pagamento" per ottenere il consenso al trattamento.
I titolari del trattamento devono inoltre valutare, caso per caso, se esiste uno squilibrio di potere tra l'individuo e il titolare del trattamento. Tra i fattori da valutare figurano la posizione delle grandi piattaforme online sul mercato, la misura in cui il singolo fa affidamento sul servizio e il pubblico principale del servizio.
Inoltre, l'EDPB fornisce elementi per valutare i criteri di consenso informato, specifico e inequivocabile di cui le grandi piattaforme online dovrebbero tenere conto nell'attuazione dei modelli "Pay or Okay".
Il presidente del comitato dei garanti europei, Anu Talus, ha inoltre raccomandato: "I titolari del trattamento dovrebbero fare sempre attenzione a evitare di trasformare il diritto fondamentale alla protezione dei dati in una funzionalità di cui gli individui devono pagare per usufruire. Gli individui dovrebbero essere resi pienamente consapevoli del valore e delle conseguenze delle loro scelte".

- N4) Sicurezza: La formazione obbligatoria e l'aggiornamento del preposto: nuova periodicità biennale dal 21/12/2023

Un approfondimento sugli obblighi relativi alla formazione del preposto e al relativo aggiornamento con riferimento alle modifiche intervenute con la legge di conversione 215/2021 del decreto-legge 146/2021. A cura dell'avvocato Rolando Dubini.

Coerentemente con la nuova e più importante posizione di garanzia del preposto, la Legge di conversione n. 215/2021 del Decreto Legge n. 146/2021 ha introdotto nell'articolo 37 del D.Lgs. n. 81/2008 sulla Formazione il nuovo comma 7-ter, ai sensi del quale "**per assicurare l'adeguatezza e la specificità della formazione nonché l'aggiornamento periodico dei preposti ai sensi del comma 7, le relative attività formative devono essere svolte interamente con modalità in presenza e devono essere ripetute, con cadenza almeno biennale** e comunque ogni qualvolta ciò sia reso necessario in ragione dell'evoluzione dei rischi o all'insorgenza di nuovi rischi".
La violazione di questo comma è punita, per il datore di lavoro e il dirigente, come da Art. 37, co. 1, 7, 7-ter, 9 e 10: **arresto da due a quattro mesi o ammenda da 1.474,21 a 6.388,23 euro** [Art. 55, co. 5, lett. c)].

Dare nuovi obblighi penalmente sanzionati al preposto, come quello di interrompere i comportamenti scorretti (articolo 19 del D.Lgs. n. 81/2008 come modificato dopo la legge 215/2021) **senza l'aggiornamento biennale della formazione non ha senso, difatti le due novità sono previste dal medesimo provvedimento normativo. Non effettuare questo aggiornamento biennale significa ledere il diritto del preposto ad aver egli strumenti per svolgere il proprio fondamentale ruolo di vigilanza così profondamente innovato nel 2021.**
Superati i due anni dello scoglio costituzionale del divieto della retroattività della norma penale, dal 21.12.2023 l'obbligo biennale è in vigore.
Il comma 7 ter non istituisce alcun collegamento tra obbligo biennale di formazione del preposto e nuovo accordo Stato Regioni, posto che restano in vigore quelli emanati a partire dal 2011.
La nota circolare INL 1/2022 che sostiene la tesi che l'obbligo di aggiornamento biennale del preposto resta in sospeso fino all'emanazione del nuovo accordo stato regioni è in contrasto con l'interpretazione letterale del comma 7 ter dell'articolo 37 quanto alla durata (a differenza di quanto previsto in precedenza, prima della legge n. 215/2021, quando si prevedeva l'aggiornamento periodico del preposto, e in tal caso non vi era dubbio che la periodicità veniva demandata all'Accordo Stato Regioni – ASR -): **ma questo aspetto era praticamente irrilevante se il nuovo Accordo Stato Regioni fosse stato emanato entro il 21 dicembre 2023.**
L'articolo 37 del D.Lgs. n. 81/2008 per la periodicità biennale dell'aggiornamento dei preposti non fa alcun riferimento al nuovo accordo Stato Regioni, quindi dal 21 dicembre 2023 (per evitare qualunque forma di retroattività della norma penale, vietata dalla Costituzione) entra direttamente in vigore secondo la tabella che pubblico più oltre, con i contenuti previsti dal vigente accordo sulla formazione.
Devo pure sottolineare, con la Suprema Corte, che le circolari dell'Amministrazione non vincolano né cittadini e aziende, né tanto meno i giudici, non costituendo fonte di diritto, e dovrebbero limitarsi a fornire indicazioni utili agli uffici preposti sul territorio per l'attuazione delle norme stesse.
Oltretutto, "la circolare ministeriale, interpretativa di una disposizione di legge, è, in linea di principio, un atto interno finalizzato ad indirizzare uniformemente l'azione degli organi amministrativi, privo di effetti esterni" (Consiglio di Stato, sez. III, 26 ottobre 2016 n. 4478). Tali atti, quindi, non solo non possono essere considerati presupposti di provvedimenti lesivi dei diritti di cittadini e aziende, di lavoratrici, lavoratori e preposti, ma addirittura gli ufficiali della P.A. che si limitano a riproporre il contenuto precettivo di atti normativi in vigore,

possono tranquillamente disattenderne l'interpretazione senza che ciò comporti l'illegittimità dei loro atti per violazione di legge (Consiglio di Stato, sez. III, 26 ottobre 2016 n. 4478).

Caso	Scadenza
Corso preposto o aggiornamento svolto prima del 21/12/2021 e con scadenza quinquennale prevista entro il 21/12/2023	Scadenza come da ASR vigente al momento del corso di formazione, ma i due anni di aggiornamento decorrono dal 21/12/2023 (data di entrata in vigore piena - non retroattiva - dell'obbligo)
Corso preposto o aggiornamento svolto prima del 21/12/2021 e con scadenza quinquennale prevista oltre il 21/12/2023	Aggiornamento entro il 21/12/2023 (entro i due anni di entrata in vigore piena – non retroattiva - dell'obbligo)
Corso preposto o aggiornamento svolto in data 21/12/2021 o successivamente.	Scadenza biennale (in questo caso non si pone il problema del divieto di retroattività)

Studio Violi è a Vostra disposizione per eventuali approfondimenti specifici in materia.

- N5) Sicurezza: Il decreto-legge 19/2024 e le novità della patente a crediti per i cantieri temporanei

Pubblicato in Gazzetta Ufficiale il Decreto-Legge 2 marzo 2024 n. 19.
Dal 1° ottobre 2024, le imprese e i lavoratori autonomi che operano nei cantieri temporanei o mobili saranno tenuti al possesso di una patente a crediti. Le indicazioni normative.

Riguardo al sistema di qualificazione, il decreto-legge 2 marzo 2024, n. 19 con l'articolo 29, comma 19, apporta importanti cambiamenti relativamente all'art. 27 del decreto legislativo 9 aprile 2008, n. 81.
Il "nuovo" articolo 27, come sostituito dal DL, **introduce un sistema di qualificazione delle imprese e dei lavoratori autonomi tramite crediti e a decorrere dal 1° ottobre 2024, le imprese e i lavoratori autonomi che operano nei cantieri temporanei o mobili saranno tenuti al possesso di una patente a crediti.**
Nel comma 1 si indica che "a far data dal 1° ottobre 2024 e all'esito della integrazione del portale di cui al comma 9, sono tenuti al possesso della patente di cui al presente articolo le imprese e i lavoratori autonomi che operano nei cantieri temporanei o mobili di cui all'articolo 89, comma 1, lettera a).
La patente è rilasciata, in formato digitale, dalla competente sede territoriale dell'Ispettorato nazionale del lavoro subordinatamente al possesso dei seguenti requisiti da parte del responsabile legale dell'impresa o del lavoratore autonomo richiedente:

a. iscrizione alla camera di commercio industria e artigianato;
b. adempimento, da parte del datore di lavoro, dei dirigenti, dei preposti e dei lavoratori dell'impresa, degli obblighi formativi di cui all'articolo 37;
c. adempimento, da parte dei lavoratori autonomi, degli obblighi formativi previsti dal presente decreto;
d. possesso del documento unico di regolarità contributiva in corso di validità (DURC);

e. possesso del Documento di Valutazione dei Rischi (DVR);
f. possesso del Documento Unico di Regolarità Fiscale (DURF).

Il comma 3 ricorda che la patente "**è dotata di un punteggio iniziale di 30 crediti e consente ai soggetti di cui al comma 1 di operare nei cantieri temporanei o mobili di cui all'articolo 89, comma 1, lettera a), con una dotazione pari o superiore a 15 crediti**".
Dunque, con una dotazione inferiore a quindici crediti non si consente alle imprese e ai lavoratori autonomi di operare nei cantieri temporanei o mobili.

Il comma 4 ricorda poi che **la patente "subisce le decurtazioni correlate alle risultanze degli accertamenti e dei conseguenti provvedimenti definitivi emanati nei confronti dei datori di lavoro, dirigenti e preposti dell'impresa o del lavoratore autonomo**:
a. accertamento delle violazioni di cui all'Allegato I: 10 crediti;
b. accertamento delle violazioni che espongono i lavoratori ai rischi indicati nell'Allegato XI: 7 crediti;
c. provvedimenti sanzionatori di cui all'articolo 3, commi 3 e seguenti, del decreto-legge 22 febbraio 2002, n. 12, convertito, con modificazioni, dalla legge 23 aprile 2002, n. 73: 5 crediti;
d. riconoscimento della responsabilità datoriale di un infortunio sul luogo di lavoro da cui sia derivata:
    1. la morte: 20 crediti;
    2. un'inabilità permanente al lavoro, assoluta o parziale: 15 crediti;
    3. un'inabilità temporanea assoluta che importi l'astensione dal lavoro per più di quaranta giorni: 10 crediti.

E "nei casi di infortuni da cui sia derivata la morte o un'inabilità permanente al lavoro, assoluta o parziale, la competente sede territoriale dell'Ispettorato nazionale del lavoro può "sospendere, in via cautelativa, la patente fino a un massimo di dodici mesi". Ed è l'ispettorato nazionale del lavoro che "definisce i criteri, le procedure e i termini del provvedimento di sospensione".

Veniamo al reintegro dei dati.
Il comma 7 ricorda che crediti decurtati "possono essere reintegrati a seguito della **frequenza, da parte del soggetto nei confronti del quale è stato emanato uno dei provvedimenti di cui ai commi 4 e 5, dei corsi di cui articolo 37, comma 7. Ciascun corso consente di riacquistare 5 crediti,** a condizione della trasmissione di copia del relativo attestato di frequenza alla competente sede dell'Ispettorato nazionale del lavoro. I crediti riacquistati ai sensi del presente comma non possono superare complessivamente il numero di quindici. Trascorsi due anni dalla notifica degli atti e dei provvedimenti di cui ai commi 4 e 5, previa trasmissione alla competente sede dell'Ispettorato nazionale del lavoro di copia dell'attestato di frequenza di uno dei corsi di cui al presente comma, la patente è incrementata di un credito per ciascun anno successivo al secondo, sino ad un massimo di dieci crediti, qualora l'impresa o il lavoratore autonomo non siano stati destinatari di ulteriori atti o provvedimenti di cui ai commi 4 e 5. Il punteggio è inoltre incrementato di cinque crediti in relazione alle imprese che adottano i modelli di organizzazione e di gestione di cui all'articolo 30".

Il comma 9 ricorda poi che le informazioni relative alla patente "confluiscono in un'apposita sezione del portale nazionale del sommerso di cui all'articolo 19 del decreto-legge 30 aprile 2022, n. 36 convertito dalla legge 29 giugno 2022, n. 79. Con decreto del Ministro del lavoro e delle politiche sociali sono individuate le modalità di presentazione della richiesta di rilascio ed i contenuti informativi della patente di cui al presente articolo".
E (comma 10) le disposizioni di cui ai commi da 1 a 9 "possono essere estese ad altri ambiti di attività individuati con decreto del Ministro del lavoro e delle politiche sociali, sulla base di quanto previsto da uno o più accordi stipulati a livello nazionale dalle organizzazioni sindacali dei datori di lavoro e dei lavoratori comparativamente più rappresentative".

Si parla anche di esoneri e il comma 11 indica che non sono tenute al possesso della patente di cui al presente articolo "le imprese in possesso dell'attestato di qualificazione SOA di cui all'articolo 100, comma 4, del codice dei contratti pubblici di cui al decreto legislativo n. 36 del 2023".

Segnaliamo anche una modifica all'articolo 90 (obblighi del committente o del responsabile dei lavori), comma 9 del D.Lgs. 81/2008, introducendo l'obbligo, introdotto con lettera b-bis), della verifica del "possesso della patente di cui all'articolo 27 nei confronti delle imprese esecutrici o dei lavoratori autonomi, anche nei casi di subappalto, ovvero, per le imprese che non sono tenute al possesso della patente ai sensi del comma 8 del medesimo articolo 27, dell'attestato di qualificazione SOA".

Voglia gradire i nostri più cordiali saluti *ing. Giorgio Violi* *ing. Alberto Sant'Unione*

PregandoLa di scusarci per il disturbo eventualmente arrecato, Le comunichiamo che i Suoi dati sono registrati nel Database Studio Violi srl e questo messaggio Le è stato inviato confidando che i temi trattati potessero essere di Suo interesse. In ottemperanza al Reg. 679/2016/UE, qualora non desiderasse più ricevere questo mensile dallo Studio Violi srl (titolare del trattamento dei dati), può comunicarcelo via mail all'indirizzo info@studiovioli.com. Garantiamo in ogni momento il rispetto di tutti i diritti di cui al Reg. 679/2016/UE.
Credits:si ringraziano le società che hanno facilitato la stesura del presente con la fornitura di parte del materiale, in particolare garante privacy, punto sicuro, ats, ipsoa, il sole24ore, tuttoambiente, iae, quotidiano sicurezza.it, privacylawconsulting, la repubblica, italia oggi, epc, postilla, necsi. Può inoltre contare sulla ns disponibilità ad approfondire i temi qui trattati