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

2003-2023
oltre vent'anni di consulenza per le imprese

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 Qualità, Ambiente, Sicurezza, Etica; servizi di consulenza in ambito Privacy, Modelli Organizzativi, Sicurezza sul lavoro, Consulenza di Direzione e sostenibilità ESG

2024 Dicembre **Il nostro punto di vista su…** *Anno 17 – 2° sem*

Periodico di informazione per i CLIENTI dello STUDIO VIOLI

Indice delle NOTIZIE (N)

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

"Il cambiamento è la legge della vita. E coloro che guardano solo al passato o al presente certamente perderanno il futuro"

John F. Kennedy (35° presidente degli Stati Uniti d'America)

“Prova pratica al corso di formazione per...Babbo Natale”

Notizie

- N1) Privacy: Software house alleate di professionisti e imprese per l'adeguamento alla privacy

I produttori di software gestionali sono responsabili del trattamento, devono fornire ai loro clienti le specifiche tecniche necessarie per dimostrare che sono conformi agli standard previsti dal Gdpr e alla cessazione del servizio devono dare ai clienti il tempo di riprendersi i dati, necessari per la continuità operativa.

Sono queste le prescrizioni più significative **del codice di condotta "privacy"** che disciplina il trattamento dei dati personali effettuato dalle **imprese di sviluppo e produzione di software gestionale, promosso da Assosoftware e approvato dal Garante della privacy con il provvedimento n. 618 del 17/10/2024, pubblicato sulla Gazzetta Ufficiale n. 278 del 27/11/2024**.

I software gestionali sono diffusissimi e riguardano tutti i processi produttivi (approvvigionamento, magazzino, vendite, fatturazione, rapporti con clienti, gestione documentale ecc.), l'attività dei professionisti (gestione dello studio, contabilità, attività tributarie, lavoristiche, legali e fiscali) e delle Amministrazioni (appalti, gestione delle gare e commesse, ecc.). Si tratta di gestionali sui quali transitano quantità enormi dati personali e per i quali si pone il problema del rispetto della normativa sulla privacy.

Il codice di condotta, ad adesione volontaria, è lo strumento previsto dall'articolo 40 del Gdpr per dettagliare in uno specifico ambito gli adempimenti previsti dalla normativa sulla protezione dei dati.

Il codice di condotta disciplina:

1) le attività di progettazione e sviluppo dei software, che di regola non comportano il trattamento di dati personali;

2) le attività di installazione, test, collaudo, assistenza, manutenzione e aggiornamento dei software gestionali, che possono comportare operazioni di trattamento di dati personali eseguite dai produttori per conto dei clienti.

In questa seconda categoria sono comprese, a titolo esemplificativo, le seguenti attività: migrazione dati finalizzata all'installazione del software, attività di assistenza e aggiornamento software con accesso da remoto, acquisizione o esportazione di copia di dati per verifica di problemi tecnici.

Il codice di condotta si applica a ciascun software gestionale per il quale il produttore presenti una richiesta di adesione.

Il codice dettaglia in un allegato (indicato con la lettera "A") le prescrizioni per l'adeguata protezione dei dati nelle attività di gestione e sviluppo.

Assistenza: chi fa cosa

Con riferimento alle attività di installazione, assistenza e manutenzione, il produttore del software, se tratta dati per conto del cliente, può assumere il ruolo e gli obblighi di responsabile del trattamento ai sensi dell'articolo 28 del Gdpr.

Se, però, il cliente della software house sia esso stesso il fornitore di un cliente finale (come nel caso, per esempio, di professionisti) e, quindi, se il cliente della software house sia già un responsabile del trattamento, in questi casi, la software house rivestirà il ruolo di "ulteriore responsabile", detto anche "sub-responsabile" (articolo 28, paragrafi 2 e 4, Gdpr).

Al riguardo il codice distingue due contesti, in cui la software house svolge la sua attività.
Può trattarsi di attività svolta in cloud: questo significa che il cliente della software house utilizza il software del produttore attraverso infrastrutture rese disponibili da quest'ultimo (direttamente o tramite suoi sub-fornitori).
Oppure può trattarsi di attività svolta on premise: in questo caso il software è installato su infrastrutture, apparati e sistemi del cliente o di fornitori di quest'ultimo.
Quando la software house agisce in cloud, questa modalità operativa le fa assumere il ruolo di responsabile del trattamento.
Quando, invece, la software house svolge tali attività on premise, essa è da considerarsi responsabile del trattamento solo quando tratta dati. Ciò può avvenire, per esempio, nelle seguenti ipotesi: 1) migrazione dati finalizzata all'installazione e al collaudo del software gestionale; 2) assistenza e aggiornamento del software gestionale con possibilità (anche occasionale) di accesso remoto ai dati del cliente (per esempio tramite strumenti di help-desk, remoto Vpn, ecc.); 3) attività di acquisizione di data base del cliente o esportazione e copia di dati personali del cliente per verificare problematiche di carattere tecnico e svolgere attività di assistenza e manutenzione.
Per i casi in cui agisce come responsabile del trattamento, il codice mette a disposizione un fac simile dell'accordo, che deve essere obbligatoriamente stipulato (articolo 28 Gdpr).
Nello schema di accordo è prevista la possibilità per il cliente di opporsi a eventuali sub fornitori individuati dalla software house, ma non si tratta di un veto, perché il mancato gradimento può portare a uno scioglimento del contratto con la software house.
Una espressa clausola è dettata per i casi in cui il subfornitore sia un soggetto con una forza contrattuale incontrastabile, rispetto al quale non c'è concreta possibilità di negoziare le modalità di erogazione del servizio.
Il codice prevede, dunque, che il produttore del software possa avvalersi di questi giganti come sub-responsabili (quali, per esempio, service providers multinazionali di servizi di hosting/data center), i quali forniscono i loro servizi sulla base di condizioni e termini contrattuali dagli stessi fissati e non trattabili, adoperandosi il più possibile ad assistere il cliente. Anche in questo caso, se il sub responsabile non è gradito, il cliente potrà sciogliersi dal contratto con la software house (ma dovrà cercarsi un altro fornitore).

Alcune clausole del codice impegnano le software house ad assistere i loro clienti (di imprese, p.a. e professionisti) nella conformità alla privacy. L'adozione di misure standard nella produzione e fornitura di software da parte dei produttori di software aderenti al codice potrà, infatti, essere usata dai clienti nella gestione degli adempimenti previsti a loro carico dal Gdpr.
In dettaglio il codice vincola i produttori di software a fornire ai loro clienti le informazioni concernenti le caratteristiche ed il funzionamento del software gestionale a livello tecnico, nonché le correlate funzionalità e misure di sicurezza: sono tutte informazioni che confluiranno nell'apparato documentale privacy del cliente.
A questo proposito il codice elenca:
1) misure tecniche e organizzative applicate dalle software house per garantire i requisiti di privacy by design e by default nelle attività di sviluppo dei software gestionali (allegato A);
2) misure di sicurezza applicate dalle software house per lo svolgimento dei servizi riguardanti i software gestionali impiegati nei contesti on premise e in cloud (allegato B).

In dettaglio, il codice stabilisce, dunque, che l'adozione, da parte del produttore del software, delle misure elencate agli allegati A e B, potrà facilitare i clienti nelle valutazioni condotte dagli stessi nella stesura di misure tecniche e organizzative (articolo 24 Gdpr), privacy by design e by default (articolo 25 Gdpr), analisi dei rischi (articolo 32 Gdpr) e valutazioni di impatto privacy (articolo 35 Gdpr). Inoltre, il riferimento contenuto negli Allegati A e B alle disposizioni applicabili del Gdpr e alle norme internazionali tecniche di rilievo, precisa il codice, permetterà al cliente di condurre autonomamente le verifiche di conformità del software gestionale rispetto alla normativa privacy.
Si cerca di semplificare la vita al cliente, il quale, verificando le misure standard applicate dalla software house, sarà facilitato nel dimostrare la propria conformità al Gdpr.

Il servizio cessa: che succede?

Un momento molto delicato del rapporto tra la software house e il cliente è la cessazione del servizio.
Il codice cerca di disinnescare ogni eventuale contenzioso, prescrivendo che, alla cessazione del servizio, il produttore del software è tenuto alla cancellazione dei dati personali dai sistemi usati per il servizio. Prima, però, di procedere alla cancellazione, il produttore del software deve mantenere a disposizione del cliente i dati personali per un periodo non inferiore a trenta giorni successivi alla cessazione del contratto: il cliente deve avere il tempo di estrarre i dati o chiedere copia secondo le modalità convenute con il produttore del software.
In effetti, i dati sono del cliente e la software house è tenuta a restituirli, affinché il cliente possa continuare a lavorare. D'altra parte, il cliente non può porre a carico delle software house onerosi adempimenti dopo la cessazione del servizio: eventuali ricadute economiche di questi profili sono lasciati alla contrattazione tra le parti.

Adempimenti Gdpr semplificati

Di diretto interesse dei produttori di software sono alcune semplificazioni relative ad adempimenti del Gdpr. Per esempio, in relazione alla tenuta e alla conservazione dei registro delle attività di trattamento, considerato che possono prestare la propria attività di responsabili del trattamento in favore di un elevato numero di clienti quali titolari, i produttori del software possono: a) indicare i clienti titolari del trattamento tramite il rinvio o il collegamento a schede o banche dati anagrafiche dei medesimi clienti, con i relativi prodotti e/o servizi acquistati; b) descrivere le categorie dei trattamenti svolti mediante rinvio a schede di servizio o a documentazione tecnica del prodotto o servizio.
Il codice è aperto alla adesione di tutti i produttori di software, anche se non associati ad Assosoftware, i quali possono presentare domanda di adesione al codice di condotta per uno o più software.

- N2) Privacy: Computer e banche dati, la password da sola non basta più: serve l'autenticazione a due fattori

Autenticazione a più fattori per accedere a computer, dispositivi e banche dati.
La password da sola non basta più.
È quanto raccomandano le Linee Guida "per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio", adottate dall' ACN, Agenzia per la Cybersicurezza Nazionale (edizione di novembre 2024).

Le Linee guida sono la risposta dell'ACN a fatti di cronaca, che hanno fatto emergere casi di accessi abusivi a banche dati di rilevanza nazionale da parte di soggetti, i quali hanno carpito informazioni e compilato report e dossier ai danni di personaggi politici e del mondo dell'economia.

Per scongiurare episodi di questo tipo, l'ACN ha elaborato un protocollo di sicurezza e un elenco di 32 misure. Il vademecum delle azioni di contrasto è articolato in sei sezioni: controllo degli accessi, buone prassi nello sviluppo di sistemi e app, gestione del ciclo di vita di sistemi e app, gestione sicurezza nell'approvvigionamento, monitoraggio e auditing e, infine, formazione del personale.

Le novità - Le linee guida in esame anticipano un più ampio catalogo di prescrizioni, che sarà definito dell'ACN ad aprile 2025, in attuazione della normativa NIS 2 (d.lgs. 138/2024). Le raccomandazioni formulate dalle linee guida riguardano tutte le banche dati di soggetti pubblici e privati e, seppure simili a quelle previste dalla normativa sulla privacy, se ne distinguono perché sono finalizzate non solo alla tutela dei dati personali, ma più in generale a garantire la continuità operativa in ambienti informatici sicuri. Peraltro, quando l'attività si riferisce anche a dati personali, norme sulla privacy e norme sulla cybersicurezza devono essere applicate cumulativamente. Di conseguenza le linee guida ACN sono un punto di riferimento anche per l'adempimento degli articoli 24, 32 e 35 Gdpr (regolamento Ue sulla privacy n. 2016/679).

La stretta sugli accessi - Scendendo nei dettagli delle misure di controllo degli accessi, oltre a una identificazione puntuale dei diversi poteri (privilegi) di accesso alle banche dati, una prescrizione invita all'adozione di sistemi di autenticazione a più fattori per l'accesso ai sistemi e alle banche dati: ad esempio, contestuale utilizzo di una password e altri elementi come password temporanee inviate via sms oppure l'impronta digitale dell'utente. Le banche dati devono, inoltre, essere protetti anche con sistemi automatizzati di allarmi in caso di accessi non autorizzati. Rimanendo sulle password, una misura, relativa allo sviluppo dei sistemi, sollecita la generazione di password casuali estremamente complesse. In quest'ultima sezione si trova anche la raccomandazione di disinstallare servizi e software non necessari. Periodici test di penetrazione dei sistemi e smaltimento sicuro dei dispositivi sono precauzioni inserite nel capitolo del ciclo di vita dei sistemi. Completano il quadro delle prescrizioni il monitoraggio dell'accesso da parte di fornitori alle banche dati con revoca delle credenziali alla cessazione della fornitura (catena di approvvigionamento), l'adozione di firewall e sistemi centralizzati di log e di rilevazione di eventi connessi a possibili minacce (auditing), corsi di cybersicurezza per il personale dotati di accessi privilegiati e di programmi di sensibilizzazione di tutto il personale (formazione).

La tabella delle 32 misure di sicurezza comprende, accanto a cautele tecniche, anche cautele fisiche (come gestione e controllo dell'accesso fisico a locali e ai dispositivi), cautele giuridiche (clausole di cybersicurezza nei contratti con i fornitori) e cautele organizzative (definizione precisa di ruoli e responsabilità per i monitoraggi).

- N3) Privacy: Consiglio di Stato: l'utente deve capire se i suoi dati sono usati per il marketing

Stop alle gincane nelle piattaforme on line: chi apre un account non deve essere costretto a vagare tra varie schermate per saper se i dati inseriti per aprire il profilo saranno usati per fini di marketing, ma deve poterlo capire subito.

Chi sparpaglia le notizie in un labirinto di link commette una pratica commerciale ingannevole.

È quanto ha stabilito il Consiglio di Stato (sezione VI, sentenza n. 9614 del 2/12/2024), la cui novità sta proprio nell'inquadrare la trasparenza sul trattamento dei dati nell'ambito della correttezza commerciale.

I dati hanno valore economico - In effetti la sentenza parte proprio dal presupposto che i dati hanno un valore economico e che, di conseguenza, si applicano anche le regole del codice del consumo (dlgs n. 206/2005) per punire slealtà e illeciti nel trattamento.

Le tutele del codice del consumo, quindi, nel caso dei dati dei consumatori, si aggiungono a quelle previste dal Gdpr (regolamento Ue sulla privacy n. 2016/679). I due comparti viaggiano coordinati, ma rimangono separati, come dimostra la sentenza in esame su un altro tema importante e cioè la preimpostazione del consenso dell'utente a ricevere comunicazioni di marketing (salvo successiva opposizione): per Palazzo Spada non si tratta di una condotta commerciale aggressiva; peraltro, se ci si sposta sul fronte "privacy" (profilo non esaminato dalla pronuncia, perché estraneo allo specifico contenzioso) il consenso "di default" è una violazione del Gdpr.

Le plurime sfaccettature di informative e consensi sono state scandagliate in una vicenda che ha coinvolto Apple e l'Autorità Garante della Concorrenza e del Mercato (Agcm).

L'Agcm ha sanzionato Apple per due violazioni (5 milioni di euro ciascuna): mancanza di trasparenza sull'uso a fini commerciali dei dati raccolti al momento della creazione dell'account Apple; preimpostazione del consenso alla raccolta dei dati a fini commerciali e imposizione di una complessa procedura per la revoca dell'assenso. Apple ha impugnato le sanzioni, che sono state entrambe annullate dal Tar Lazio.

L'Agcm ha presentato appello al Consiglio di Stato, che ha salvato solo la prima sanzione. Per arrivare a questo esito, la pronuncia afferma che è di natura commerciale la decisione di fornire i propri dati personali (proprio perché hanno un valore economico) quando si apre un account su una piattaforma digitale (articolo 18, comma 1, lett. m), codice del consumo), anche se l'apertura non sia effettuata nel contesto di atti di acquisto. Simmetricamente, la sentenza afferma che è una pratica commerciale la procedura allestita da una piattaforma, che consente agli utenti di creare account, anche se il servizio fornito all'utente è gratuito (articolo 18, comma 1, lett. d), codice del consumo).

Ma se queste ipotesi sono comprese in un quadro commerciale, allora, va considerata quale pratica commerciale ingannevole la mancanza di chiarezza e trasparenza sull'utilizzo dei dati (articolo 22 del codice del consumo). E, in effetti, il Consiglio di Stato ha salvato la sanzione irrogata dall'Antitrust a Apple, rea di non avere specificato, fin dall'inizio della procedura di creazione dell'account, del possibile utilizzo dei dati per l'invio

di messaggi promozionali "personalizzati": non basta, chiarisce la sentenza, un'informativa "multilivello" con un giro tortuoso di link per poter sapere come stanno le cose.

Al contrario, è stata salvato dalla censura di aggressività commerciale (articolo 25 del codice del consumo), il consenso a ricevere proposte commerciali quale impostazione predefinita: la pronuncia non lo ritiene oppressivo e neppure manipolatorio della volontà, anche quando per la revoca del consenso l'utente è costretto a seguire un iter complesso. Tutto ciò, beninteso, ai sensi degli articoli 25 e 26 del codice del consumo. Al riguardo, infatti, si deve sottolineare un profilo ulteriore rispetto ai temi trattati dalla pronuncia e cioè che il consenso di default costituisce una grave violazione dell'articolo 7 del Gdpr, punita con una pesante sanzione pecuniaria.

- N4) Ambiente: RENTRI - Modalità, soggetti obbligati e scadenze

Il RENTRI è il Registro Elettronico Nazionale sulla Tracciabilità dei Rifiuti che rappresenta una vera e propria rivoluzione nella gestione ambientale di migliaia di aziende,

poiché permetterà la tracciabilità dei rifiuti attraverso un modello di gestione digitale per l'assolvimento degli adempimenti ambientali quali **l'emissione dei formulari di identificazione del trasporto e la tenuta dei registri cronologici di carico e scarico.**
Quanto ai termini per l'iscrizione è stata prevista una partenza a scaglioni.

Già a decorrere dal 15 dicembre 2024 ed entro il 13 febbraio 2025 sono iniziate le iscrizioni per il primo gruppo di soggetti obbligati, ossia per le imprese produttori iniziali di rifiuti speciali pericolosi e non pericolosi con più di 50 dipendenti, e per tutti gli altri soggetti diversi dai produttori iniziali, ivi incluse le associazioni imprenditoriali.

Enti o imprese produttori di rifiuti speciali pericolosi e non pericolosi **con più di 10 dipendenti** (secondo gruppo di soggetti obbligati) **avranno tempo per iscriversi dal 15 giugno 2025 ed entro il 14 agosto 2025**,

mentre **tutti i restanti produttori iniziali di rifiuti** speciali pericolosi (terzo gruppo di soggetti obbligati) dovranno iscriversi a decorrere **dal 15 dicembre 2025 ed entro il 13 febbraio 2026**.

In ogni caso, a prescindere dall'obbligo di iscrizione al RENTRI, **dal 13 febbraio 2025 dovranno essere utilizzati i nuovi modelli di registro di carico e scarico e formulario**.
Per tutti e tre i gruppi di soggetti obbligati, **dal 13 febbraio 2026 i formulari diventeranno digitali**.

- N5) Sicurezza: Approvato in Senato il DDL Lavoro 2024: tutte le novità per la sicurezza sul lavoro e le modifiche al Decreto 81/2008

L'11 dicembre 2024 è stato definitivamente approvato il disegno di legge di iniziativa governativa in titolo recante "Disposizioni in materia di lavoro" o DDL Lavoro 2024.
Il disegno di legge risulta composto da 34 articoli.

1) Sorveglianza sanitaria e ruolo del medico competente: le novità del Decreto lavoro 2024

All'interno del DDL Lavoro molte previsioni riguardano la figura del medico competente e le visite da esso svolte. In particolare, con riferimento alla sorveglianza sanitaria dei lavoratori (articolo 1) si prevede:

- **Elenco Medici competenti di salute e sicurezza sul lavoro:** richiesto aggiornamento da parte del Ministero Lavoro in base alla verifica periodica del requisito specifico inerente all'educazione continua in medicina;
- **visita medica preventiva in fase preassuntiva:** costituirà una delle modalità di adempimento dell'obbligo di visita medica preventiva intesa a constatare l'assenza di controindicazioni al lavoro;
- **visita preassuntiva**: eliminata la possibilità che sia svolta (su scelta del datore di lavoro) dal dipartimento di prevenzione dell'azienda sanitaria locale, anziché dal medico competente, e che quest'ultimo, nella prescrizione di esami ritenuti necessari in sede di visita preventiva, tenga conto delle risultanze dei medesimi esami e indagini già effettuati dal lavoratore al fine di evitarne la ripetizione, qualora lo ritenga compatibile con le finalità della visita preventiva;
- **visita medica precedente alla ripresa del lavoro dopo assenza per malattia superiore a 60 giorni**: l'obbligo sussiste solo qualora la visita sia ritenuta necessaria dal medico competente. Qualora questi non ritenga necessario procedere alla visita, è tenuto a dichiararlo tramite il rilascio di apposito giudizio di idoneità alla ripresa della mansione specifica;
- **Accordo tossicodipendenza e dell'alcoldipendenza**: entro il 31 dicembre 2024 la consultazione delle parti sociali, in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano;
- **ricorsi contro i giudizi del medico competente**: l'autorità competente sarà l'azienda sanitaria locale

2) Lavori in locali chiusi sotterranei/semisotterranei

Il DDL Lavoro 2024 prevede una modifica delle condizioni alle quali è subordinato lo svolgimento di lavori in locali chiusi sotterranei o semisotterranei, tra l'altro sopprimendo la condizione della sussistenza di particolari "esigenze tecniche" e definendo una procedura amministrativa unica per la possibilità delle lavorazioni nei locali in oggetto.

3) Cantieri edili: tessere personali

Il DDL Lavoro 2024 mira ad abrogare alcune norme relative agli obblighi inerenti alle tessere personali di riconoscimento nei cantieri edili, in considerazione del fatto che tale disciplina è stata successivamente definita dal D.Lgs. 81 del 2008, che, con riferimento a tutte le attività svolte in regime di appalto o subappalto, a prescindere dalla sussistenza o meno di un cantiere edile, richiede che i datori di lavoro muniscano i lavoratori dipendenti delle suddette tessere e che i medesimi lavoratori, nonché i lavoratori autonomi, tengano esposte tali tessere sul luogo di lavoro.

4) Stato di salute e sicurezza del Paese: nuovo obbligo per il Ministero Lavoro

Il Disegno di legge Lavoro prevede anche che il Ministero del lavoro e delle politiche sociali rediga una Relazione annuale sullo stato della sicurezza nei luoghi di lavoro, sugli interventi da adottare e sugli orientamenti e i programmi legislativi che il Governo intende prendere al riguardo per l'anno in corso, da presentare alle Camere entro il 30 aprile di ciascun anno con riferimento all'anno precedente.

5) Assicurazione infortuni e malattie professionali

Nell'articolo 2 c'è poi spazio per le modifiche alla disciplina per la definizione dei ricorsi in materia di applicazione delle tariffe dei premi per l'assicurazione contro gli infortuni sul lavoro e le malattie professionali.
Inoltre, si richiede che anche l'INAIL possa recuperare le somme indebitamente versate dallo stesso Istituto successivamente al decesso dei beneficiari (articolo 3);
Il DDL prevede anche la modifica alla disciplina dei ricorsi in materia di prestazioni dell'assicurazione contro gli infortuni in ambito domestico, prevedendo che gli stessi siano decisi dalla sede INAIL che ha emesso il provvedimento ritenuto illegittimo e non più dal comitato amministratore del Fondo autonomo speciale istituito ad hoc per la gestione delle prestazioni Inail in favore dei suddetti lavoratori domestici (articolo 4);
Infine, il DDL Lavoro 2024 prevede che, dal 1° gennaio 2025, le comunicazioni di decesso trasmesse all'INPS, siano messe a disposizione dell'INAIL (articolo 5).

- Chiusura per festività e Auguri

Questo Natale Studio Violi ha voluto esprimere la propria vicinanza e solidarietà alle persone in difficoltà attraverso il sostegno ad associazioni locali e nazionali: Caritas Diocesana di Carpi, Fondazione IEO-MONZINO, Ageop Bologna.

Si comunica che lo Studio chiuderà per le festività natalizie da lunedì 23 Dicembre 2024 a lunedì 6 Gennaio 2025 compresi e riaprirà regolarmente martedì 07 Gennaio 2025.

Per necessità urgenti è possibile scrivere una mail a givioli@gmail.com indicando un recapito telefonico e il contenuto della richiesta.
Cercheremo di rispondervi rapidamente, considerando comunque la possibilità che non sia possibile dare riscontro urgentemente.

L'occasione è gradita per formulare i migliori auguri di un Santo e sereno Natale 2024 e di buon inizio del nuovo anno 2025.

ing. Giorgio Violi ing. Alberto Sant'Unione