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 Novembre **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

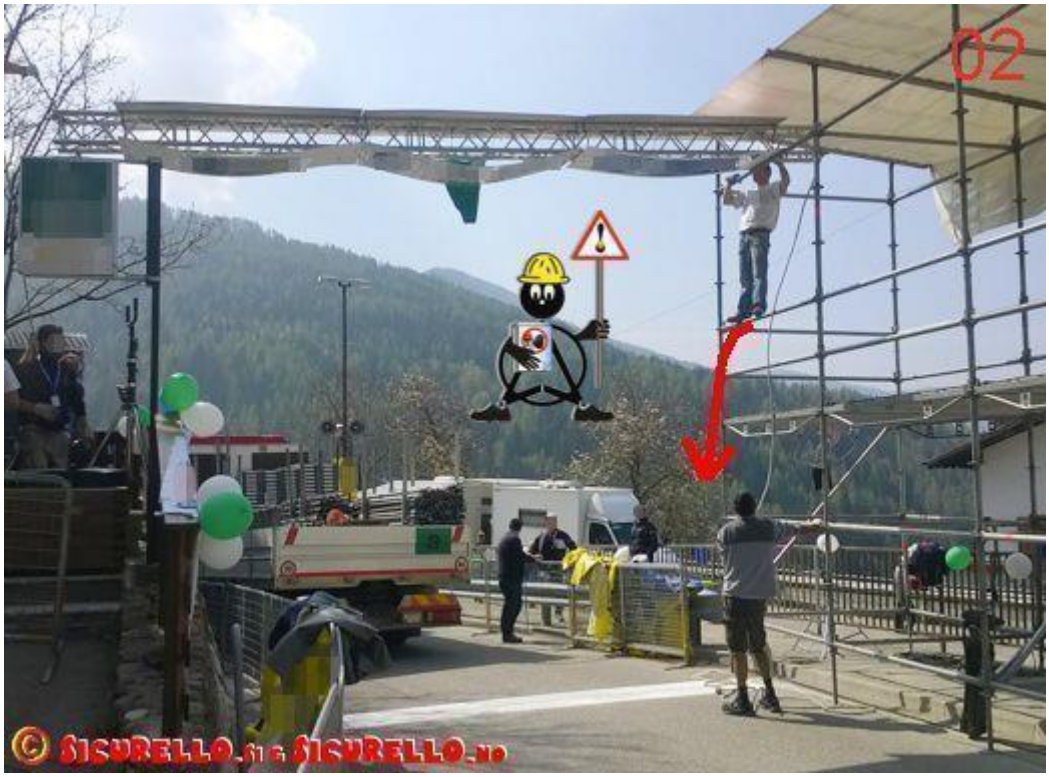
- Sul sito http://www.dottrinalavoro.it/argomento/giurisprudenza-c/corte-di-cassazione-c sono presenti le ultime sentenze di Cassazione relative al lavoro

AFORISMA DEL MESE

"Open mind for a different view
And nothing else matters"

James Hetfield (cantautore, chitarrista e compositore statunitense)

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



“Interferenze? Caduta dall’alto? Altro?”

Notizie

- N1) Sicurezza: Formazione dei preposti, il Ministero del Lavoro risponde sulla periodicità (5 anni)

In attesa del nuovo Accordo Stato-Regioni sulla formazione, i preposti della sicurezza sul lavoro in azienda dovranno continuare ad aggiornarsi ogni 5 anni.

A chiarirlo è il **Ministero del Lavoro nell'interpello n. 6 del 24 ottobre 2024**, rispondendo a un quesito sulla formazione dei preposti, ossia i soggetti incaricati, secondo il Testo unico sulla sicurezza (Dlgs 81/2008), di sovrintendere e vigilare sul rispetto da parte dei lavoratori degli obblighi di legge e delle disposizioni aziendali in materia di sicurezza e utilizzo dei dispositivi di protezione.

Il Ministero specifica che le novità introdotte dall'articolo 37, comma 7-ter del Dlgs 81/2008, il quale prevede che la formazione dei preposti in ambito di sicurezza debba essere rinnovata almeno ogni 2 anni, dipendono dall'adozione del nuovo Accordo Stato-Regioni in materia di formazione, ancora in bozza nella versione del maggio 2024 (doveva essere approvato il 7 novembre scorso ma poi è stata rinviata l'approvazione).

Come confermato anche dalla circolare n. 1/2022 dell'Ispettorato nazionale del lavoro, fino all'entrata in vigore delle nuove disposizioni l'aggiornamento continuerà a seguire la cadenza quinquennale, secondo quanto previsto dall'Accordo Stato-Regioni del 21 dicembre 2011, n. 221.

- N2) Sicurezza: Interpello n. 4/2024: ruolo e identificazione del preposto nelle piccole imprese

L'Interpello n. 4/2024 emesso dalla Commissione per gli interpelli in materia di salute e sicurezza sul lavoro del Ministero del Lavoro e delle Politiche Sociali, chiarisce l'obbligatorietà e l'individuazione del preposto nelle piccole imprese e realtà con un solo lavoratore.

La Commissione evidenzia l'importanza del ruolo del preposto come garante della sicurezza, confermando l'obbligatorietà della sua individuazione e citando precedenti interpelli per rafforzare la sua posizione.
Nelle piccole realtà aziendali, il preposto può coincidere con il datore di lavoro, ma solo come ultima opzione, dopo aver valutato l'organizzazione aziendale e **limitatamente ai casi in cui il datore di lavoro supervisioni direttamente l'attività**. In un'impresa individuale, il datore di lavoro assume automaticamente le funzioni di preposto, non potendo il lavoratore unico ricoprire tale ruolo su sé stesso.
I datori di lavoro, sia appaltatori che subappaltatori, devono indicare al committente chi tra il personale ricopre il ruolo di preposto, assicurandosi che questa persona possa effettivamente adempiere alle responsabilità del ruolo, anche in termini di presenza fisica sul luogo di lavoro.
La normativa citata nell'interpello riguarda il ruolo del preposto e le sue responsabilità, includendo la supervisione diretta di operazioni critiche come l'installazione di ponteggi.
In conclusione, l'Interpello 4/2024 delinea chiaramente l'importanza del preposto nel contesto lavorativo, particolarmente in contesti di piccola scala, e stabilisce linee guida per la sua corretta identificazione e funzione.

- N3) Sicurezza: Denunce di infortuni e malattie professionali – i dati INAIL dei primi nove mesi del 2024

Le denunce di infortunio nei primi nove mesi del 2024 sono state 433.002 (+0,5%), con un aumento dei soli incidenti avvenuti in itinere. I casi mortali sono stati 776 (+2,0%). In aumento del 22% le patologie di origine professionale denunciate, pari a 65.000.

Le denunce di infortunio presentate all'Inail nei primi nove mesi del 2024 sono state 433.002, in aumento dello 0,5% rispetto alle 430.829 dello stesso periodo del 2023, del 9,2% rispetto a gennaio-settembre 2021 e del 18,1% rispetto a gennaio-settembre 2020, e in diminuzione del 19,2% sul 2022 e del 7,6% sul 2019, anno che precede la crisi pandemica. Tenendo conto dei dati sul mercato del lavoro rilevati mensilmente dall'Istat nei vari anni, con ultimo aggiornamento settembre 2024, e rapportando il numero degli infortuni denunciati a quello degli occupati (dati provvisori), si evidenzia un'incidenza infortunistica che passa da 2.032 denunce di infortunio ogni 100mila occupati Istat del 2019 a 1.805 del 2024, con un calo dell'11,1%. Rispetto al 2023 la riduzione è dello 0,8% (da 1.819 a 1.805).

Tra i settori con i maggiori incrementi dei casi avvenuti in occasione di lavoro si evidenziano l'Istruzione (+46,9%), la Sanità e assistenza sociale (+25,1%), la Riparazione, manutenzione e installazione di macchine e apparecchiature (+18,8%), la Fornitura di acqua-reti fognarie, attività di gestione dei rifiuti e risanamento (+16,2%), il Noleggio e servizi di supporto alle imprese (+14,8%), le Attività dei servizi di alloggio e di ristorazione (+13,2%) e le Costruzioni (+11,6%).

L'analisi territoriale evidenzia un aumento delle denunce nelle Isole (+2,3%), seguite da Centro (+1,2%), Nord-Ovest (+0,6%), Nord-Est (+0,1%), e un calo al Sud (-0,7%). Tra le regioni con i maggiori incrementi percentuali si segnalano le province autonome di Trento (+14,8%) e Bolzano (+4,5%), l'Umbria (+3,9%), la Sicilia (+3,1%) e la Calabria (+2,6%), mentre per i decrementi la Basilicata (-5,4%), l'Abruzzo (-4,2%), l'Emilia Romagna (-1,8%) e la Valle d'Aosta (-1,6%).

L'aumento delle denunce di infortunio che emerge dal confronto dei primi nove mesi del 2023 e del 2024 è legato soprattutto alla componente femminile che registra un +1,4% (da 150.363 a 152.435 casi denunciati), mentre quella maschile presenta una sostanziale stabilità (da 280.466 a 280.567, +0,04%). L'incremento ha interessato esclusivamente i lavoratori extracomunitari (+5,5%), in calo il dato degli italiani (-0,3%) e dei comunitari (-4,7%).

L'analisi per classi di età mostra aumenti tra gli under 15 (+20,6%), soprattutto per l'incremento degli infortuni tra gli studenti (effetto dell'estensione assicurativa Inail disposta dal decreto-legge lavoro n. 48/2023), nella fascia 20-29 anni (+1,7%) **e in quella 60-74 anni (+5,5%).** Si registra, per contro, un calo tra i 15-19enni (-2,6%), tra i 30-59enni (-2,7%) e tra gli over 74 (-1,3%).

Le denunce di malattia professionale protocollate dall'Inail nei primi nove mesi del 2024 sono state 65.333, 11.778 in più rispetto allo stesso periodo del 2023 (+22,0%). L'aumento è del 48,7% rispetto al 2022, del 61,4% sul 2021, del 106,1% sul 2020 e del 44,7% sul 2019.

I dati rilevati a settembre di ciascun anno mostrano incrementi delle patologie denunciate **nelle gestioni Industria e servizi (+22,2%, da 44.332 a 54.177 casi),** Agricoltura (+21,6%, da 8.732 a 10.621) e Conto Stato (+9,0%, da 491 a 535). L'aumento interessa il Sud (+31,2%), le Isole (+27,0%), il Centro (+20,8%), il Nord-Ovest (+14,9%) e il Nord-Est (+13,5%).

In ottica di genere si rilevano 8.947 denunce di malattia professionale in più per i lavoratori, da 39.372 a 48.319 (+22,7%), e 2.831 in più per le lavoratrici, da 14.183 a 17.014 (+20,0%). L'aumento ha interessato sia le denunce dei lavoratori italiani, che sono passate da 49.216 a 59.752 (+21,4%), sia quelle dei comunitari, da 1.337 a 1.736 (+29,8%) e degli extracomunitari, da 3.002 a 3.845 (+28,1%).

Le patologie del sistema osteo-muscolare e del tessuto connettivo, quelle del sistema nervoso e dell'orecchio continuano a rappresentare, anche nei primi nove mesi del 2024, le prime tre tipologie di malattie professionali denunciate, seguite dai tumori e dalle patologie del sistema respiratorio.

- N4) Ambiente: Immodificabilità del registro cronologico di carico e scarico digitale tramite il sistema RENTRI

La caratteristica di immodificabilità del registro riguarda la disciplina sulla formazione, gestione e conservazione dei documenti informatici; a questo proposito è opportuna una breve nota introduttiva per favorirne la contestualizzazione.

Innanzitutto, è necessario distinguere tra le annotazioni cronologiche, che devono essere effettuate nei tempi stabiliti dall'art. 190 del D.lgs. 152/2006, ed il registro, in quanto documento informatico.

E' fondamentale tenere in considerazione che il Registro cronologico di carico e scarico, nella formulazione del DM 59/2023, **è un "documento informatico" e come tale, deve formarsi nel rispetto delle linee guida definite da AgID** così come esplicitato all'art.4 del DM 59/2023 nonché di una serie di riferimenti normativi che disciplinano la tenuta di registri obbligatori con strumenti informatici che per comodità sono stati riportati al paragrafo 17.3 (requisiti generali) delle modalità operative.

Fatta questa premessa l'immodificabilità è riferita al registro cronologico "prodotto con sistemi meccanografici" che nell'ambito del RENTRI si materializza nel file XML del registro cronologico predisposto secondo i modelli XSD pubblicati nel portale RENTRI. Il file, prodotto dai servizi di supporto o dai sistemi gestionali, rappresenta il registro che l'impresa è tenuta ad esibire come stabilito dall'art 7 commi 4-ter e 4-quater dal Decreto Legge 10 giugno 1994 n.357.

Ovviamente le registrazioni andranno effettuate nel rispetto dei tempi fissati dall'art.190 del D.lgs. 152/2006.

Il formato del file XML prodotto (vedi modelli XSD del Registro C/S RENTRI disponibili nell'area Servizi per l'interoperabilità del portale RENTRI) è nativamente strutturato per garantirne l'immodificabilità. Infatti, il registro cronologico in formato XML secondo lo schema XSD definito in RENTRI prevede già una firma a chiusura di ogni ciclo di esportazione, appositamente al fine di blindare tutto il pacchetto di dati esportato (per questo motivo tale firma può essere considerata "firma tecnica"). In fase di formazione è opportuno che la firma a chiusura di ogni export XML del registro sia riconducibile alla titolarità del registro o sia una firma qualificata, per quanto si tratti solo di una sottoscrizione tecnica.

In subordine, trattandosi di una firma tecnica, l'utilizzo del certificato digitale di tipo sigillo elettronico rilasciato dal RENTRI rappresenta una possibile soluzione alternativa.

In merito alle tempistiche per rendere immodificabile il registro si precisa che è l'impresa stessa a decidere di "produrre" il registro digitale, nel formato xml, con la frequenza che riterrà idonea in base alla propria organizzazione, ed in funzione della migliore diligenza che riterrà di adottare.

Di seguito alcune ipotesi gestionali che vanno considerate valide:

Ipotesi a): nei termini previsti dalla normativa sulla conservazione delle scritture contabili (3 mesi dal termine di presentazione delle relative dichiarazioni annuali dell'esercizio di competenza),

Ipotesi b): contestualmente alla trasmissione dei dati al RENTRI (con cadenza definita nel decreto 4 Aprile 2023 n. 59)

Ipotesi c): con cadenza definita dalle procedure adottate dall'operatore (ma comunque entro i temini previsti di cui all'ipotesi a).

A prescindere dalle tempistiche che l'organizzazione intenderà seguire, in caso di ispezione da parte degli enti di controllo, l'organizzazione dovrà produrre, attraverso il sistema gestionale o attraverso i servizi di supporto, il registro da esibire.

Il versamento definitivo del registro al sistema per la conservazione a norma, di cui l'operatore ha scelto di avvalersi, eseguito con la frequenza scelta dall'impresa, e comunque almeno una volta all'anno richiederà, ai fini dell'opponibilità a terzi, la sottoscrizione digitale da parte del responsabile alla conservazione (nelle varie accezioni consentite dalla norma e secondo quanto previsto dal manuale di conservazione dell'operatore) e l'apposizione della marca temporale.

Si aggiunge che, come previsto dalla regolamentazione tecnica in materia di tenuta e conservazione dei registri, laddove l'operatore, in base a proprie scelte di natura organizzativa, intenda archiviare il file, che rappresenta il registro elettronico, prima del trasferimento al sistema di conservazione a norma, il medesimo file dovrà essere firmato digitalmente con firma qualificata.

A tal proposito si rammenta che il certificato digitale di tipo sigillo elettronico rilasciato dal RENTRI non può assolvere alla funzione di firma qualificata.

- N5) Privacy: Per lo sviluppo sostenibile dell'intelligenza artificiale serve la fiducia degli utenti, il rispetto della privacy, e il coraggio delle autorità

Lo sviluppo sostenibile della governance dei dati si sta rivelando sempre più un presupposto fondamentale per il successo della transizione digitale, e specialmente con le potenzialità dell'intelligenza artificiale è necessario che essa sia al servizio dell'uomo, e non viceversa.

Di ciò, non devono esserne convinti solo i regolatori e gli addetti ai lavori, ma occorre che si instauri un clima di fiducia generale da parte della comunità, e gli utenti devono poter percepire i vantaggi e l'affidabilità di cui possono godere avvalendosi di soluzioni di intelligenza artificiale.

Se l'utente che si trova a interagire con un robot lo percepisse solo come un ostacolo, o addirittura come qualcosa a cui egli si deve adeguare o sottomettere, l'inevitabile conseguenza sarebbe che cercherebbe di aggirarlo e di trovare soluzioni alternative.

L'Unione Europea è consapevole di questa necessità, e uno degli **scopi del nuovo Regolamento sull'intelligenza artificiale (Artificial Intelligence Act) è proprio quello di rafforzare la fiducia dei cittadini**, i quali devono essere messi in condizione di poter credere che grazie all'intelligenza artificiale potranno realmente fruire di un'assistenza sanitaria migliore, di trasporti più sicuri, servizi più efficienti, ed altri vantaggi, ma devono avere anche la certezza che tali innovazioni tecnologiche non vadano a discapito dei loro diritti fondamentali, compreso quelli riguardanti la privacy, e senza che nessuno rischi di rimanere escluso.

A tal proposito, i risultati di uno studio condotto da Federprivacy non sono però rassicuranti, perché esaminando un campione di 400 siti web di lingua italiana di vari settori di organizzazioni pubbliche e private, è stato riscontrato che il 98,7% dei siti non tende affatto la mano a coloro che hanno svantaggi sotto il profilo linguistico, culturale, e neanche alle persone con disabilità sensoriali.

Le aziende italiane fanno quindi bene a cercare di cogliere le opportunità dell'intelligenza artificiale, ma devono ponderare bene i loro investimenti: secondo un recente rapporto della società di ricerche Gartner, almeno il 30% dei progetti di intelligenza artificiale generativa verrà infatti abbandonato entro la fine del 2025. Le cause principali di questi fallimenti includono la scarsa qualità dei dati, controlli dei rischi inadeguati, costi crescenti e un valore aziendale poco chiaro.
Per evitare che la corsa all'oro dell'AI non risulti una delusione e un bagno di sangue per le imprese, è quindi necessario che i progetti non si concentrino solo sugli aspetti tecnologici, ma tengano conto anche di tutti gli altri fattori connessi, compreso il rispetto dei diritti sulla privacy degli interessati, affinché i loro investimenti abbiano un approccio sostenibile e possano guadagnare la necessaria fiducia degli utenti.

Per realizzare uno sviluppo sostenibile dell'intelligenza artificiale, nei prossimi anni un ruolo cruciale sarà giocato anche dalle autorità per la protezione dei dati, in particolare perché le sanzioni amministrative previste dal GDPR non si sono rivelate effettivamente "dissuasive" come era il proposito dell'art.83 del Regolamento europeo sulla privacy.

Efficaci e realmente dissuasive sembrano invece essersi rivelate azioni coraggiose (anche se talvolta impopolari) come quella del Garante italiano che lo scorso anno bloccò i trattamenti effettuati da OpenAI, la società americana che ha sviluppato e gestisce ChatGPT, e in effetti l'imposizione di misure severe che comportino divieti dei trattamenti illeciti come previsto dall'art. 58 par.1 lett.f) del GDPR, come pure l'introduzione di norme penali che aprano le porte del carcere per coloro che deliberatamente compiono ripetutamente gravi violazioni della normativa, potrebbero rappresentare un tassello importante per lo sviluppo sostenibile della nuova civiltà digitale.

- N6) Privacy: TikTok sanzionato per 3,5 milioni di euro dal Garante della privacy di San Marino; Indicazioni applicative emergenti sulla determinazione delle sanzioni per violazioni privacy

TikTok sanzionato per 3,5 milioni di euro dal Garante della privacy di San Marino. L'Autorità garante per la protezione dei dati personali di San Marino ha multato la piattaforma TikTok per 3,5 milioni di euro. Il provvedimento, firmato dal presidente Umberto Rapetto, è del 4 luglio scorso, ma è stato pubblicato recentemente sul sito del Garante sammarinese della privacy, ed è stato adottato dall'Autorità nei confronti di TikTok Pte Limited, la società con sede a Singapore, titolare dell'omonimo social network, tra i più in voga tra gli adolescenti.
L'Autorità sammarinese ha ritenuto che la società cui fa capo TikTok, responsabile del trattamento dei dati, non abbia adottato "alcuna idonea modalità di verifica e rilevazione circa eventuali dichiarazioni mendaci rese dall'utente in fase di registrazione e accesso alla piattaforma e, pertanto, il titolare del trattamento non risulta essersi adoperato per verificare adeguatamente che il consenso sia prestato o autorizzato da utenti maggiori di anni 16, o - in caso di utenti minori di anni 16 - dal titolare della potestà genitoriale sul minore".
E "che – si legge – non essendo adottato alcun sistema di verifica dell'età dell'utente in fase di registrazione, lo stesso, anche se di età giovanissima, può agevolmente accedere ad ogni contenuto della piattaforma con conseguenze e rischi potenzialmente di estrema gravità. Inoltre, in difetto di qualsivoglia valido consenso, i dati personali dei più giovani vengono resi accessibili da parte di terzi".
Non è la prima volta che il garante sammarinese bacchetta un gigante tecnologico, in quanto a gennaio dello scorso anno aveva vinto una battaglia legale contro Meta Inc., che dopo essere stata sanzionata per 4 milioni di euro dall'autorità guidata da Rapetto aveva deciso di fare ricorso dinanzi al Tribunale e poi alla Corte d'Appello di San Marino, dove aveva però si era vista confermare in via definitiva la multa con sentenza n° 3 del 25 gennaio 2023.

Indicazioni applicative emergenti sulla determinazione delle sanzioni per violazioni privacy. Il Provvedimento del Garante n. 306 del 23 maggio 2024 afferente un data breach nell'utilizzo della posta elettronica consente di rilevare come nell'attività del Garante a tutela della riservatezza dei dati personali emergano criteri per parametrare gli interventi sanzionatori.

Su questa materia, come pure a suo tempo trattato sul portale dell'Associazione, l'EDPB con le Linee guida 4/2022 ha fornito criteri per l'applicazione delle sanzioni; tale documento è complementare alle Linee guida WP253 (LG253) che si soffermano sulle circostanze per la quali la sanzione amministrative possa essere uno strumento di rigore più appropriato rispetto alle altre misure di rigore a disposizione della Autorità Garanti.

Il processo delineato dalle Linee guida 4/2002 prevede vari step, tenendo conto dei criteri dell'art. 83 del GDPR quali: gravità della violazione; dimensione e natura del soggetto; presenza di aggravanti e attenuanti, effettività, proporzionalità e dissuasione.

Un punto che l'EDPB, sulla base del GDPR, rimanda – per alcuni aspetti alle Autorità di controllo, per altri ai singoli Stati - è quello delle sanzioni per le entità pubbliche, fra cui la possibilità di tarare l'importo delle sanzioni per tali entità, ove previste dagli ordinamenti in relazione alla loro dimensione.

Su tale aspetto rileva in generale il punto 10 delle Linee guida 4/2022 e in particolare, la sezione 4.3 afferente alla irrogazione di una sanzione pecuniaria effettiva, dissuasiva e proporzionata in funzione del fatturato delle organizzazioni interessate. Tale sezione 4.3 è riferita elettivamente alle organizzazioni private, peraltro l'EDPB afferma che "Le autorità di controllo rimangono comunque libere di applicare una metodologia simile a quella descritta in tale sezione".

Per completezza, si rammenta che il capitolo sul "Limite massimo di legge e responsabilità delle imprese" non è applicabile al calcolo delle sanzioni pecuniarie da infliggere a entità pubbliche nel caso in cui l'ordinamento nazionale preveda limiti massimi di legge diversi e l'autorità pubblica o l'organismo pubblico non agisca come impresa.

Ad oggi sia il Provvedimento 306/2024 sia altri Provvedimenti del Garante permettono di rilevare alcune interessanti indicazioni in merito al percorso definitorio del dimensionamento delle sanzioni:

- in alcuni Provvedimenti, infatti, si menziona la tabella 1 del Manuale ENISA WP2017 0- 2-2-5 circa la misurazione dell'impatto di una violazione privacy, come nel Provvedimento n. 500 del 26 ottobre 2023;
- in altri, inerenti a soggetti pubblici, il punto 60 delle predette Linee guida 4/2022, afferente al calcolo dell'"importo iniziale adeguato" per la sanzione in relazione al livello (basso, medio o alto) da considerare poi per la determinazione finale ai sensi del punto 43, come nel Provvedimento n. 235 dell'11 aprile 2024;
- in altri ancora, come nel citato Provvedimento n. 306/2024 e in quello n. 500 del 26 ottobre 2023, entrambe tali disposizioni.

Dal consolidamento nel tempo di questi pronunciamenti – fatta salva nel frattempo la formalizzazione e pubblicizzazione della metodologia ventilata dall'EDPB - sarà possibile trarre delle linee orientative sulla procedura sanzionatoria, a beneficio di tutti i soggetti dell'ecosistema privacy.

Una particolarità che sembra emergere è quella della applicazione (sebbene a livello fattuale) dei fattori di dimensionamento delle sanzioni del paragrafo 43 delle ripetute Linee guida 4/2022 anche al settore pubblico oltre che a quello privato (cfr ad esempio l'importo della sanzione di cui al Provvedimento 235/2024).

Con riguardo alle indicazioni ENISA va per completezza indicato che il Garante italiano evidenzia:

- ad es. nel Provvedimento n. 197 del 17 maggio 2023, che per il calcolo della gravità dell'evento ha anche fatto riferimento alle Raccomandazioni ENISA del 2013 "for a methodology of the assessment of severity of personal data breaches";
- di aver collaborato alla elaborazione dello strumento strumento che ENISA ha messo a disposizione per la valutazione del rischio sicurezza.

In conclusione, il percorso verso una procedura per la gestione delle violazioni del GDPR e del Codice privacy sta proseguendo e ciò consentirà a tutti gli operatori del settore poter apprezzare la portata delle violazioni sia a fini di ottimale gestione anche del rischio privacy, nell'ambito del più generale risk management e anche nel settore pubblico.

E ciò dovrebbe avvenire non solo nel senso (deteriore) di valutare il rischio di una eventuale non compliance a fronte dei vantaggi per i propri business, ma di valorizzare il plus di fiducia e reputazionale che riviene dalla minimizzazione dei rischi per gli interessati. Che poi, non va dimenticato, potranno sempre ricercare in sede civile un risarcimento per la lesione alla propia riservatezza che ritenessero di aver subito.

- Pillole di privacy recenti

Non commette violazione della privacy l'investigatore privato che indaga sul dipendente che usa il permesso sindacale per interessi personali

Licenziato il lavoratore che usa il permesso sindacale per motivi personali. Il detective ingaggiato dall'azienda che lo accerta non commette alcuna violazione della privacy perché il controllo che gli è stato affidato risulta eseguito in luoghi pubblici e serve ad accertare le cause effettive della richiesta di permesso

Se il capo usa la password della sua collaboratrice commette reato di accesso abusivo ad un sistema informatico

Con la sentenza 40295/2024, la Cassazione si è pronunciata chiarendo l'ambito di applicazione del reato di "*accesso abusivo ad un sistema informatico*" all'interno di un rapporto di lavoro, nella fattispecie in cui un responsabile si era fatto dare da un'impiegata a lui gerarchicamente subordinata le credenziali di accesso al sistema informatico aziendale.

L'Europa si prepara all'applicazione della direttiva NIS2: ma le norme da sole non bastano

Il 17 ottobre la Commissione UE ha approvato un importante atto di esecuzione in tema di cybersicurezza, tuttavia, in molti Paesi membri dell'Unione si registra una significativa carenza di competenze nel settore, con una domanda di esperti che supera di gran lunga l'offerta.

Trasferimento dati Ue-Usa: il Comitato europeo per la protezione dei dati adotta la prima revisione del Data Privacy Framework

Nel corso della sessione plenaria del 4 novembre 2024, il Comitato europeo per la protezione dei dati (European Data Protection Board) ha adottato un rapporto sulla prima revisione del Data Privacy Framework per il trasferimento dei dati tra Unione Europea e Stati Uniti.

Commette reato di interferenze illecite il marito che registra di nascosto moglie e suocero

Compie il reato di interferenze illecite nella vita privata il marito che registra in casa propria la conversazione della moglie con un altro, ad esempio il suocero. Affinché si consumi il delitto è sufficiente che chi carpisce le voci altrui con lo smartphone non partecipi al dialogo che avviene all'interno dell'abitazione.

Garante privacy: creata task force interdipartimentale sul fenomeno degli accessi abusivi alle banche dati pubbliche e private

Dati rubati, Garante privacy: Creata task force interdipartimentale. Stanzione: *"Il fenomeno degli accessi abusivi alle banche dati pubbliche e private è da sempre all'attenzione del Garante per la protezione dei dati personali, e negli anni è stato oggetto di numerosi provvedimenti volti ad innalzare le misure di sicurezza sia da un punto di vista tecnico che organizzativo".*

tratte da Federprivacy

Voglia gradire i nostri più cordiali saluti

ing. Giorgio Violi ing. Alberto Sant'Unione