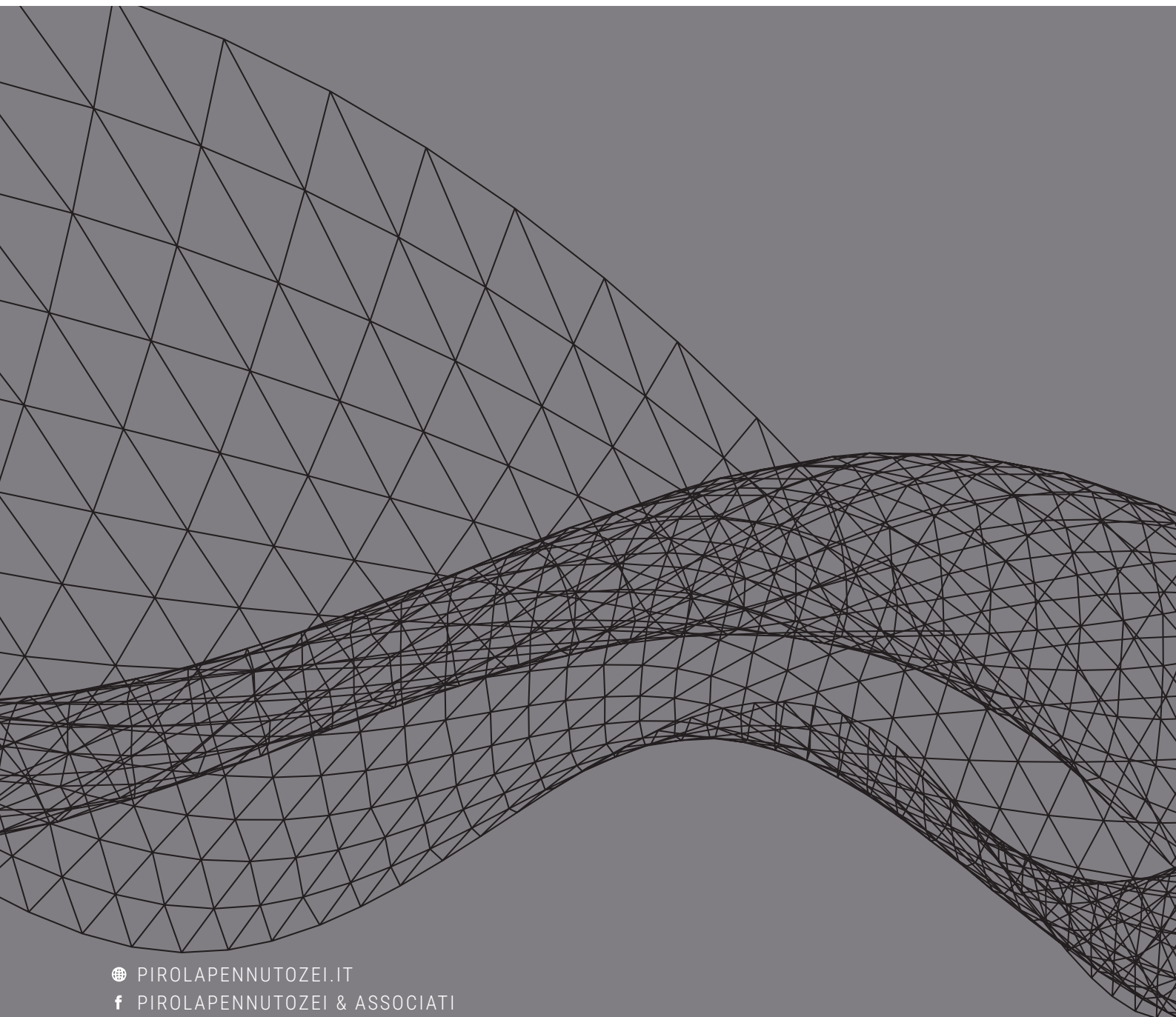


Pirola
Pennuto
Zei
& Associati
studio di consulenza
tributaria e legale

COMPLIANCE

NEWSLETTER / LUGLIO 2019



🌐 PIROLAPENNUTOZEI.IT
f [PIROLAPENNUTOZEI & ASSOCIATI](#)
t [@STUDIO_PIROLA](#)
in [PIROLA PENNUTO ZEI & ASSOCIATI](#)

NORMATIVA

1.1.....	4
Entra in vigore la Direttiva UE sul riutilizzo delle informazioni nel settore pubblico	
1.2.....	4
Il disegno di legge sul perimetro di sicurezza nazionale cibernetica: le novità per gli operatori del settore	

PRASSI

2.1.....	6
<i>European Data Protection Board</i> : pubblicate le linee guida sulla videosorveglianza	
2.2.....	6
Banca d'Italia e Procura di Milano insieme nella lotta ai reati in ambito finanziario	
2.3.....	7
Il Garante revisiona le autorizzazioni generali sul trattamento di categorie particolari di dati	
2.4.....	7
L'ANAC pubblica il nuovo rapporto sulle imprese destinatarie di interdittive antimafia	

GIURISPRUDENZA

3.1.....	9
<i>British Airways</i> : multa da 183 milioni di sterline per <i>Data Breach</i>	



INDICE

3.2	9
Cassazione: non sono necessari i gravi indizi per il sequestro preventivo	
3.3	10
Prescrizione dell'illecito e rinvio a giudizio: irrilevante la notificazione	
3.4	10
Morti bianche e adeguatezza del Modello: la pronuncia della Cassazione	

NORMATIVA

1.1

Entra in vigore la Direttiva UE sul riutilizzo delle informazioni nel settore pubblico

Il 16 luglio scorso è entrata in vigore la *"Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico"*, volta a promuovere l'utilizzo degli open data a livello comunitario e ad incentivare l'innovazione di prodotti e servizi.

La Direttiva detta gli standard minimi in materia di riutilizzo dei dati e una serie di *best practices* per agevolarlo.

Le norme vertono, in particolare, sui documenti in possesso degli enti pubblici degli Stati Membri, ma anche su quelli in possesso di soggetti privati denominati *"imprese pubbliche"*, quali: vettori aerei, compagnie di trasporto marittimo e società che erogano servizi nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, le cui attività siano finanziate in modo maggioritario dallo Stato o da altri enti pubblici, o la cui gestione sia soggetta al controllo di questi ultimi.

I documenti in questione, ai sensi della Direttiva, debbono essere riutilizzabili sia a fini commerciali che a fini non commerciali, ove possibile in formati aperti, leggibili meccanicamente, accessibili, reperibili e riutilizzabili, insieme ai rispettivi metadati.

Gli Stati Membri dovranno adeguarsi alla Direttiva 2019/1024 entro il 17 luglio 2021.

1.2

Il disegno di legge sul perimetro di sicurezza nazionale cibernetica: le novità per gli operatori del settore

Il Consiglio dei Ministri il 19 luglio scorso ha approvato il *"Disegno di legge in materia di perimetro di sicurezza nazionale cibernetica"*, volto a garantire *"un elevato livello di sicurezza delle reti, dei sistemi informativi, e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende una funzione essenziale dello Stato dal cui malfunzionamento o interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale"* (art. 1).

La formulazione in oggetto è molto ampia e, soprattutto, non fornisce ulteriori precisazioni in merito alla definizione di *"operatori nazionali privati"*. In particolare, il Disegno di Legge sarebbe applicabile a tali

operatori qualora *“esercitino una funzione essenziale dello stato, ovvero assicurino un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello stato”*, nella misura in cui *“l’esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi, e servizi informatici”*.

In assenza di maggiori indicazioni, si può supporre che la categoria comprenderà aziende di importanza strategica per la sicurezza nazionale e la difesa, quali, a titolo esemplificativo: società che erogano energia elettrica, acqua, gas e idrocarburi; grandi istituti bancari e finanziari; società che gestiscono infrastrutture (informatiche e non); ecc.

Quanto al contenuto, il DDL prevede la predisposizione di numerose misure di *cybersecurity* relative a: politiche di sicurezza, gestione del rischio, prevenzione, mitigazione e gestione di incidenti, integrità delle reti e dei sistemi informativi e molti altri ambiti.

PRASSI

2.1

European Data Protection Board: pubblicate le linee guida sulla videosorveglianza

Lo *European Data Protection Board* (EDPB), l'organo composto da rappresentanti delle Autorità di Controllo degli Stati Membri dell'UE, ha adottato il 10 luglio scorso le Linee guida 3/2019 sul trattamento dei dati personali effettuato attraverso strumenti di videosorveglianza, che chiariscono l'applicazione del Regolamento n. 679/2016 (RGPD) all'ambito della videosorveglianza, con riferimento sia ai dispositivi video tradizionali, che a quelli "*intelligenti*" (e.g. tecnologia biometrica).

Le Linee guida si applicano a tutti gli apparati di videosorveglianza che raccolgono i dati delle persone che entrano nello spazio monitorato dagli stessi, ponendo una particolare attenzione sul trattamento ulteriore delle immagini effettuato al fine di verificare la presenza ed il comportamento degli individui ripresi.

L'EDPB ha chiarito che, prima ancora di mettere in funzione una telecamera, il Titolare del trattamento (pubblico o privato che sia) deve valutare dove e quando è strettamente necessario adottare misure di videosorveglianza e che la misura in questione sia proporzionata alla finalità perseguita, operando un bilanciamento con gli interessi, i diritti e le libertà fondamentali degli interessati.

Le basi giuridiche del trattamento, in linea generale, sono quelle disciplinate dagli artt. 6, par. 1, lett. e) RGPD – "*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*" – e 6, par. 1, lett. f) RGPD – "*il trattamento è necessario per il perseguimento del legittimo interesse del titolare o di terzi*".

Le Linee guida sono ora soggette a consultazione pubblica; tale fase terminerà il 9 agosto 2019.

2.2

Banca d'Italia e Procura di Milano insieme nella lotta ai reati in ambito finanziario

Lo scorso 19 luglio il Procuratore della Repubblica presso il Tribunale di Milano, Francesco Greco, e il Governatore della Banca d'Italia, Ignazio Visco, hanno firmato un Protocollo d'Intesa volto a rafforzare la cooperazione tra le due istituzioni e ad incrementare lo scambio di informazioni.

Il Protocollo è mirato a contrastare la criminalità in ambito finanziario, con specifico riferimento ai reati di riciclaggio, autoriciclaggio e finanziamento del terrorismo.

In particolare, la Banca d'Italia si impegna a dare comunicazione alla Procura ogniqualvolta accerti

fattispecie di possibile rilievo penale nello svolgimento delle proprie attività. Al contempo, *Palazzo Koch* potrà richiedere alla Procura informazioni relative a procedimenti penali rilevanti nell'ambito dell'attività di vigilanza.

Il Protocollo d'Intesa assume rilievo nel contesto della responsabilità amministrativa dell'ente in quanto i reati di riciclaggio e autoriciclaggio e i delitti con finalità di terrorismo sono reati presupposto ai sensi degli artt. 25-*octies* e 25-*quater* del D.lgs. 231/2001. Alla luce del Protocollo, quindi, è ragionevole aspettarsi un rafforzamento dell'attività ispettiva nell'ambito dei reati di cui sopra.

2.3

Il Garante revisiona le autorizzazioni generali sul trattamento di categorie particolari di dati

È in corso di pubblicazione sulla Gazzetta Ufficiale il "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101*", n. 9124510, del 5 giugno scorso, con il quale il Garante ha portato a termine l'opera di revisione delle Autorizzazioni generali disposta dal d.lgs. 101/2018.

Il Provvedimento detta gli obblighi da rispettare nel trattamento di categorie particolari di dati in specifici contesti e in particolare: nei trattamenti svolti nell'ambito di rapporti di lavoro; nei trattamenti relativi all'attività di organismi di tipo associativo, fondazioni, chiese e associazioni o comunità religiose; nei trattamenti compiuti da investigatori privati; nei trattamenti di dati genetici; e, infine, nei trattamenti ai fini di ricerca scientifica.

2.4

L'ANAC pubblica il nuovo rapporto sulle imprese destinatarie di interdittive antimafia

Lo scorso 8 luglio l'Autorità Nazionale Anticorruzione ha pubblicato il rapporto "*Le imprese destinatarie di interdittive antimafia (2014-2018)*", che evidenzia un significativo aumento delle interdittive - cioè le misure applicate nei confronti di aziende nelle quali si sono registrate infiltrazioni mafiose - nel periodo di riferimento.

In totale, nei quattro anni in esame, 2.044 imprese hanno ricevuto interdittive antimafia, emesse dall'ANAC stessa o dalle Prefetture territoriali. Il report dà contezza di una crescita "*costante e generalizzata in ogni zona del Paese*".

L'Autorità ravvisa la causa principale di tali evidenze numeriche innanzitutto in un miglioramento dei



PRASSI

flussi informativi, dovuto al virtuosismo ed alla diligenza delle Prefetture. Al contempo, l'ANAC ravvisa quale concausa la sempre più penetrante attività investigativa dell'Autorità giudiziaria, che fornisce alle Prefetture informazioni di vitale importanza per la disamina dei profili antimafia.

GIURISPRUDENZA

3.1

British Airways: multa da 183 milioni di sterline per Data Breach

L'8 luglio scorso l'*Information Commitioner's Office* (ICO), ovvero l'Autorità di Controllo per il Regno Unito, ha annunciato al *London Stock Exchange* l'intenzione di comminare una sanzione di 183 milioni di sterline (204 milioni di Euro) per violazioni delle norme del GDPR a carico di *British Airways*, in relazione alla *Data Breach* subita l'anno passato.

La compagnia di bandiera UK, infatti, l'estate scorsa aveva subito un cyberattacco che aveva causato la violazione dei dati personali di all'incirca 500.000 passeggeri, provenienti da tutto il mondo. Gli utenti del sito internet di *British Airways*, infatti, venivano sistematicamente deviati verso un sito fraudolento che ne raccoglieva dati personali quali credenziali di accesso a siti web e app della compagnia, dati anagrafici, dati di contatto, prenotazioni e dettagli di viaggio, e dati di carte di pagamento.

Nonostante la compagnia si sia attivata immediatamente, notificando la violazione secondo le tempistiche dettate dall'art. 33 del Regolamento (72 ore dal momento in cui ne è venuta a conoscenza) e mettendo in atto misure volte a contenere i danni, l'ICO ha ritenuto di comminare una sanzione esemplare, a causa delle scarse misure di sicurezza dei dati implementate all'epoca dei fatti.

La sanzione prevista dall'ICO corrisponde all'1,5% del fatturato globale annuo di *British Airways*, ed è quindi pienamente in linea con il dettato del Regolamento (art. 83 par. 4).

L'ammontare definitivo, in ogni caso, sarà determinato solamente a seguito di una consultazione con le Autorità di Controllo degli altri Stati Membri coinvolti nella violazione e preso atto delle ulteriori dichiarazioni che la compagnia aerea britannica addurrà a propria difesa.

3.2

Cassazione: non sono necessari i gravi indizi per il sequestro preventivo

La Corte di Cassazione è tornata a pronunciarsi sul dibattuto tema del sequestro preventivo a carico di società in relazione a illeciti ambientali. Con la Sentenza n. 31232, depositata lo scorso 16 luglio, la Corte ha dichiarato che *“in tema di sequestro preventivo, non è necessario valutare la sussistenza dei gravi indizi di colpevolezza a carico del soggetto nei cui confronti è operato il sequestro, essendo sufficiente che sussista il fumus commissi delicti, vale a dire la astratta sussumibilità in una determinata ipotesi di reato del fatto contestato [...], sicché il giudice può rilevare anche il difetto dell'elemento soggettivo del reato purché esso emerga ictu oculi, cioè sia di immediato rilievo”*.

La vicenda riguardava ingenti quantità di rifiuti, che erano stati interrati senza prima essere trattati, come richiesto dalla normativa di settore.

Nel caso di specie, due società, appartenenti al medesimo gruppo, si erano viste contestare la commissione dell'illecito di cui all'art. 25-*undecies* del d.lgs. 231/2001 ("*Reati ambientali*"), per aver consentito a soggetti apicali la commissione del reato di traffico organizzato di rifiuti ex Art. 452-*quaterdecies cod.pen.*.

Il GIP, alla luce dei rilievi preliminari, aveva disposto il sequestro preventivo finalizzato alla confisca per equivalente dei beni aziendali, fino a concorrenza del profitto conseguito. Tale misura cautelare era stata confermata dal Tribunale della libertà di Bari in sede di riesame. Di conseguenza, i ricorrenti avevano adito la Cassazione, lamentando vizi processuali e assenza di motivazione.

Gli Ermellini hanno rigettato il ricorso, ritenendo il *fumus commissi delicti* elemento sufficiente a fondamento del sequestro preventivo, sottolineando anche la mancata adozione di un Modello di organizzazione, gestione e controllo da parte delle società. La Corte ha anche precisato, però, che i profili relativi alla insussistenza di gravi indizi, seppur non utili ai fini dell'opposizione al sequestro preventivo, possono essere dedotti nei casi in cui essi siano talmente evidenti da rendere illogico il provvedimento cautelare.

3.3

Prescrizione dell'illecito e rinvio a giudizio: irrilevante la notificazione

Il 12 luglio scorso la Corte di Cassazione ha depositato la sentenza n. 30634 con la quale ha chiarito la disciplina degli atti interruttivi della prescrizione per gli illeciti amministrativi a carico degli enti.

Il procedimento in esame verteva, nel merito, su un infortunio sul luogo di lavoro. In prima istanza, il Tribunale di Rimini aveva dichiarato il non luogo a procedere per sopravvenuta prescrizione dell'illecito amministrativo dovuto alla tardiva notificazione del decreto di rinvio a giudizio. Il P.M. ricorreva quindi in Cassazione avverso la pronuncia del giudice di merito.

Gli Ermellini hanno confermato che la notificazione della richiesta di rinvio a giudizio "*in quanto atto di contestazione dell'illecito, interrompe, per il solo fatto della sua emissione, la prescrizione e ne sospende il decorso dei termini fino al passaggio in giudicato della sentenza che definisce il giudizio*".

3.4

Morti bianche e adeguatezza del Modello: la pronuncia della Cassazione

Con la sentenza n. 29538 depositata lo scorso 8 luglio la Corte di Cassazione è tornata ad esprimersi

sulla correlazione fra morti sul luogo di lavoro e inefficace attuazione del Modello di organizzazione, gestione e controllo ex d.lgs. 231/2001.

Il caso in parola riguardava un operaio esperto, che, a seguito della rimozione del dispositivo di sicurezza di un macchinario per la verniciatura "a nastro", aveva avuto accesso ad una zona pericolosa per verificare un difetto ed era rimasto incastrato con il braccio nei rulli, con conseguente distacco dell'arto e successivo decesso.

Il GUP di Cremona, in prima istanza, aveva assolto i soggetti apicali coinvolti nel procedimento, nonché l'ente stesso. Il Procuratore della Repubblica aveva proposto ricorso avverso tale pronuncia presso la Corte di Appello di Brescia, che aveva, invece, condannato i convenuti. Questi ultimi hanno quindi adito la Corte di Cassazione.

Gli Ermellini, accogliendo la posizione della Corte bresciana, hanno rigettato i ricorsi. La Cassazione ha ravvisato la sussistenza della responsabilità a carico dei soggetti apicali ritenendo che *"l'operatività dei sistemi di protezione deve risultare vincolante per il lavoratore, nel senso che essa non va lasciata alla buona volontà o alla perfetta attenzione di questi e che la loro rimozione non dev'essere consentita in modo semplice e immediato, sì che il lavoratore sia quantomeno 'dissuasivo' dal neutralizzarli"*. Di conseguenza, nonostante la rimozione dei dispositivi di sicurezza per la verifica di difetti non fosse pratica invalsa all'interno dello stabilimento, la responsabilità dei sopracitati soggetti discende dal fatto che l'operaio aveva avuto la possibilità di rimuovere con facilità, seppur parzialmente, un presidio di sicurezza.

Per quanto riguarda la società, invece, la Corte ha ravvisato una responsabilità derivante dalla inefficace attuazione del Modello di organizzazione, gestione e controllo, in violazione dell'art. 6, comma 1, lett. a), poiché, *"pur essendosi provveduto all'analisi dei rischi con riferimento all'impianto di verniciatura e, segnatamente, all'attività dei capi turno, l'istruzione operativa predisposta era incompleta [...] rispetto alle modalità di ricerca e soluzione dei difetti sul nastro (l'attività, per l'appunto, che stava svolgendo la vittima nell'occorso)"*.

La Cassazione ha anche rilevato l'inadeguatezza dell'operato dell'Organismo di Vigilanza, il quale non aveva provveduto a svolgere le attività propedeutiche a tale monitoraggio a causa di ritardi aziendali.

Altri indici della inefficace attuazione del Modello ravvisati dalla Corte sono il mancato svolgimento di attività di audit e i *"ritardi nella esecuzione delle attività previste dall'Action Plan (in particolare, nella redazione delle procedure per effettuare i controlli, poiché l'avvio delle attività di verifica in materia di salute e sicurezza era stata pianificata per il febbraio 2015)"*.

COMPLIANCE NEWSLETTER | LUGLIO 2019

RIFERIMENTI NORMATIVI, PRASSI E GIURISPRUDENZA AL 31 LUGLIO 2019.

LA PRESENTE NEWSLETTER ILLUSTRATA LE PRINCIPALI NOVITÀ E ALCUNE QUESTIONI DI INTERESSE GENERALE, E RAPPRESENTA DUNQUE UNO STRUMENTO MERAMENTE INFORMATIVO, IL CUI CONTENUTO NON VA UTILIZZATO COME BASE PER EVENTUALI DECISIONI OPERATIVE.

PER ULTERIORI INFORMAZIONI, VI INVITIAMO A CONTATTARE IL VOSTRO PARTNER DI RIFERIMENTO O AD INVIARE UN'EMAIL A UFFICIOSTUDI@STUDIOPIROLA.COM