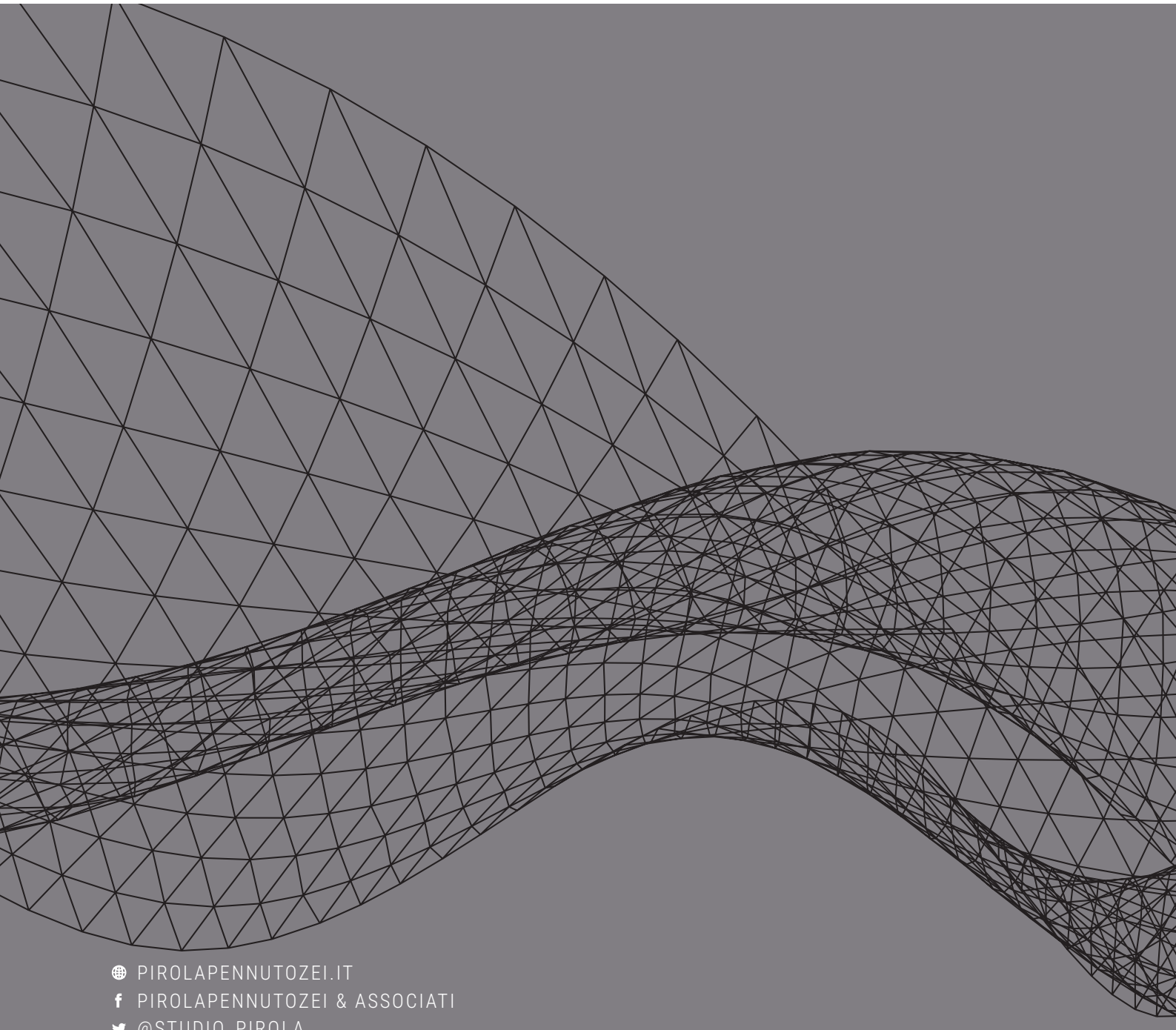
Pirola
Pennuto
Zei
& Associati

studio di consulenza
tributaria e legale

COMPLIANCE

NEWSLETTER / SETTEMBRE 2019



PIROLAPENNUTOZEI.IT
PIROLAPENNUTOZEI & ASSOCIATI
@STUDIO_PIROLA
PIROLA PENNUTO ZEI & ASSOCIATI

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDICE

NORMATIVA

PRASSI

GIURISPRUDENZA

TORNA ALL'INDICE ↑

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDICE

NORMATIVA

1.1

La Germania compie un altro passo verso la responsabilità da reato degli enti

Il Ministero della Giustizia tedesco ha recentemente pubblicato un disegno di legge in materia responsabilità da reato delle imprese.

Il documento, concettualmente evocativo del D.Lgs. 231/2001, mira ad introdurre un sistema sanzionatorio rivolto alle società per i reati commessi dai soggetti apicali, nonché una serie di incentivi per lo svolgimento di *audit* interni e ad operare una revisione complessiva della disciplina in materia di perquisizioni e sequestri.

Come già avviene con riferimento ai modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001, il disegno di legge prevede che l'adozione di un "*compliance program*" adeguato possa comportare una sostanziale riduzione delle sanzioni.

La normativa introduce sanzioni pecuniarie significative che potranno raggiungere fino al 10% della media del fatturato annuo dei tre anni fiscali precedenti all'illecito per le aziende con un fatturato annuo di € 100 milioni.

E' previsto un principio di extraterritorialità nell'applicazione della legge per i casi in cui i reati, pur commessi fuori dal territorio tedesco, siano riconducibili ad un'impresa domiciliata in Germania.

1.2

In vigore il Decreto Legge in materia di perimetro nazionale di cibersicurezza con un nuovo reato presupposto

Lo scorso 22 settembre è stato pubblicato in Gazzetta Ufficiale il Decreto Legge 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*".

L'atto introduce un nuovo reato presupposto nell'ambito della responsabilità amministrativa degli enti ex D.Lgs. 231/2001.

Il D.L., emanato anche alla luce delle preoccupazioni circa la realizzazione dell'infrastruttura 5G in Italia, è 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*", delegando ad ulteriori provvedimenti

la definizione puntuale dei requisiti tecnici, dei soggetti ricompresi nel perimetro e delle modalità di applicazione.
Il D.L. introduce una nuova fattispecie rilevante ai fini della responsabilità amministrativa degli enti ex D.Lgs. 231/2001, per la quale chiunque, allo scopo di ostacolare o condizionare l'espletamento degli adempimenti di: 1) predisposizione e aggiornamento con cadenza almeno annuale di elenchi di reti, sistemi informativi e servizi informatici; 2) procedure per la concessione di forniture di servizi ICT di cui sopra; o 3) attività di ispezione e verifica sul rispetto delle disposizioni del D.L. da parte delle Autorità Competenti, fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per l'attuazione dei predetti adempimenti, o omette di comunicare entro i termini tali informazioni, "è *punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote*".

1.3

La Camera approva la responsabilità giuridica degli enti per le frodi IVA

Il 1 ottobre scorso la Camera dei Deputati ha approvato in via definitiva la Legge di delegazione europea 2018, che delega al Governo anche il recepimento della "*Direttiva (UE) 2017/1371 del Parlamento Europeo e del Consiglio del 5 luglio 2017 relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale*" (c.d. "*Direttiva PIF*").
La Direttiva prescrive l'istituzione della responsabilità in capo agli enti per i reati gravi commessi a danno del sistema IVA, ovverosia nei casi in cui la condotta delittuosa sia connessa "*al territorio di due o più Stati membri dell'Unione e comport(i) un danno complessivo pari ad almeno 10.000.000 EUR*".
A fronte dell'obbligo di recepimento di tale disciplina, il Legislatore ha ritenuto di delegare al Governo tale adempimento, da sostanziarsi tramite l'individuazione dei reati ritenuti lesivi degli interessi finanziari dell'UE e delle relative pene, l'abrogazione delle norme incompatibili e l'integrazione del D.Lgs. 231/2001.
La Direttiva, in ogni caso, indica a titolo esemplificativo alcune sanzioni la cui applicazione in capo alle persone giuridiche è ritenuta appropriata, quali, ad esempio "*l'esclusione temporanea o permanente dalle procedure di gara pubblica, l'interdizione temporanea o permanente di esercitare un'attività commerciale e la chiusura temporanea o permanente degli stabilimenti che sono stati usati per commettere il reato*" (art. 9) oltre che il congelamento e la confisca degli strumenti utilizzati per commettere i reati e dei proventi derivanti dagli stessi (art. 10).
Il Governo dovrà provvedere ad emanare apposito atto legislativo entro tre mesi dalla data di entrata in vigore della Legge di delegazione europea 2018.

PRASSI

2.1

Il Garante della Privacy approva il nuovo codice di condotta per i sistemi di informazione creditizia

Il Garante per la Protezione dei Dati Personali ha approvato con il Provvedimento n. 9141941 del 12 settembre scorso il nuovo "*Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti*", che recepisce le novità legislative introdotte dal GDPR.

Il nuovo Codice di condotta è focalizzato su alcuni settori di importanza strategica, quali mutui, prestiti, noleggio, leasing, prestiti gestiti via Fintech. Il Garante, ha infatti dichiarato che: "*al fine di favorire il corretto funzionamento del mercato finanziario e creditizio, i dati censiti potranno essere trattati senza il consenso degli interessati, sulla base del cosiddetto legittimo interesse delle società partecipanti ai Sic (Sistemi di informazioni creditizie), garantendo però i più ampi diritti previsti dal Regolamento europeo in materia di protezione dei dati*".

Il Codice, in tale contesto, pone un particolare accento sul principio di minimizzazione dei dati di cui all'art. 5 del GDPR, secondo il quale i dati personali devono essere adeguati, pertinenti e limitati rispetto alle finalità – in questo caso – di valutazione del rischio creditizio.

Inoltre, viene introdotto l'obbligo per coloro che gestiscono Sic di verificare ed aggiornare periodicamente – con cadenza perlomeno biennale – i modelli di analisi statistica, così come gli algoritmi utilizzati.

GIURISPRUDENZA

3.1
Multa da 660.000 euro a Morele.net per violazione del principio di integrità e riservatezza dei dati personali

L'Autorità polacca per la protezione dei dati personali ("*UODO*") ha irrogato la sanzione più alta fino ad oggi per violazione delle norme in materia di protezione dei dati personali, per un ammontare complessivo di 660.000 euro. La maxi-multa è stata comminata lo scorso 19 settembre in capo alla società Morele.net, un *online retailer,* in conseguenza ad una violazione dei dati personali dei propri clienti risalente al dicembre dell'anno scorso.
Il *data breach* ha comportato il furto di nomi, indirizzi e-mail e di consegna e numeri di telefono di circa 2,2 milioni di utenti tramite tecniche di *phishing.*
La società ha provveduto a notificare il *data breach* alle Autorità e agli interessati entro le tempistiche richieste dal GDPR, ma l'indagine seguita ha evidenziato che le misure tecniche e organizzative adottate da Morele.net fossero inadeguate.
In particolare, l'online retailer non avrebbe rispettato il principio di integrità e riservatezza di cui all'art. 5, par. 1, lett. f) del GDPR, secondo il quale i dati personali devono essere "*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*".
Inoltre, l'UODO ha contestato a Morele.net di non aver monitorato efficacemente le potenziali minacce ai dati personali, non avendo quest'ultima reagito con sufficiente tempestività nel momento in cui si è resa conto che massicce quantità di dati personali erano in fase di *download.*

3.2
ANAC: irrogata la prima sanzione per violazione del divieto di atti di ritorsione nei confronti del *whistleblower*

Durante l'Adunanza del 4 settembre scorso, con la Delibera n. 782, l'Autorità Nazionale Anticorruzione ha irrogato per la prima volta una sanzione per violazione del divieto di atti di ritorsione nei confronti del *whistleblower.*
La controversia verteva su una denuncia mossa all'Autorità Giudiziaria da un dirigente di un Comune campano nei confronti di alcuni dipendenti dell'Ufficio Procedimenti Disciplinari (UPD) dello stesso, per i reati di abuso d'ufficio ed omissione di atti d'ufficio, a seguito dell'archiviazione da parte di questi ultimi di

un procedimento disciplinare relativo ad atti di violenza verbale subiti dal dirigente stesso. Il segnalante era stato successivamente sospeso dal servizio con privazione della retribuzione. Inoltre, al *whistleblower* era stata contestata la violazione del codice di comportamento del Comune, che imponeva di segnalare eventuali illeciti – in via riservata – in primo luogo al Responsabile della Prevenzione della Corruzione.
Nel corso dei procedimenti disciplinari era stata negata al segnalante la tutela di cui all'art. 54-*bis* del D.Lgs. 165/2001 ("*Tutela del dipendente pubblico che segnala illeciti*"), poiché l'anonimato era stato ritenuto essenziale per la qualifica di *whistleblower*.
L'ANAC, deliberando sulla complessa diatriba, ha posto in risalto il fatto che "*non è certamente vero che il whistleblower è solo colui che segnala condotte illecite in forma anonima*".
Inoltre, l'Autorità ha dichiarato che il fatto che il segnalante fosse obbligato a denunciare i fatti a norma del Codice Penale e del Codice di Procedura Penale non pregiudica la qualifica in capo allo stesso di whistleblower, in quanto l'art. 54-*bis* del D.Lgs. 165/2001 "*presenta un ambito soggettivo e oggettivo più ampio*" rispetto alle norme contenute in tali codici.

3.3

Corte di Giustizia UE: il diritto all'oblio non si estende oltre i confini dell'Unione

Lo scorso 24 settembre, con la sentenza n. C-507/17, la Corte di Lussemburgo ha sancito che il diritto all'oblio si applica unicamente al territorio dell'UE, mentre al di fuori di questo i dati personali possono continuare ad essere visualizzati liberamente.
Il caso in esame scaturisce da un'istanza mossa dal Presidente del "*Commission Nationale de l'Informatique et des Libertés*" (c.d. "*CNIL*") – il Garante della privacy francese – nei confronti di Google, la quale è stata condannata a pagare una multa da 100.000 euro per la mancata eliminazione di dati personali a seguito della richiesta di esercizio del diritto all'oblio da tutti i domini del proprio motore di ricerca. A fronte di tale sanzione, Google aveva adito il "*Conseil d'État*", richiedendo l'annullamento della pronuncia del Garante.
Il "*Conseil d'État*", quindi, si era rivolto alla Corte di Giustizia UE, domandando se l'operatore di un motore di ricerca debba eliminare i dati personali da tutte le versioni del proprio motore di ricerca – anche quelle extra-UE – oppure se l'eliminazione dei dati debba essere invece limitata alle versioni del motore di ricerca corrispondenti a ciascuno Stato membro dell'UE.
La Corte di Giustizia, osservando che molti Stati al di fuori dell'Unione non contemplano il diritto all'oblio, e che il diritto alla protezione dei dati personali non è un diritto assoluto, ma bensì è da considerarsi in relazione alla sua funzione sociale e da bilanciarsi con altri diritti fondamentali, ha concluso affermando

che la legislazione europea non prevede l'obbligo di applicare il diritto all'oblio a tutte le versioni del proprio motore di ricerca, ma solo negli Stati membri dell'Unione.

3.4

Tar Puglia: se il DPO è una persona giuridica, il preposto dev'essere un suo dipendente

Il Tar di Lecce si è recentemente pronunciato in merito alla figura del Responsabile della Protezione dei Dati personali (noto anche come "*RPD*" o "*DPO*"), apportando un interessante spunto al dibattito dottrinale sul ruolo e sulle funzioni di tale carica. Con la sentenza n. 1468/2019 – pubblicata il 13 settembre scorso – difatti, la Corte pugliese ha stabilito che, nell'eventualità in cui un Titolare o un Responsabile del trattamento decida di assegnare l'incarico di DPO ad una società, la persona fisica che effettivamente ricopre il ruolo dev'essere necessariamente un dipendente di quest'ultima.
Il caso in esame verteva su un ricorso presentato avverso la graduatoria finale di una gara d'appalto indetta dal Comune di Taranto per la nomina del DPO. Il primo classificato, difatti, era una società che aveva indicato quale persona fisica effettivamente deputata a ricoprire il ruolo un individuo legato alla stessa dalla prestazione di un incarico professionale e non di dipendente.
Il Tribunale, prendendo a fondamento della propria decisione le "*Linee guida sui responsabili della protezione dei dati" del 13 dicembre 2016, ha stabilito che "la persona fisica che svolge funzioni di RPD, quando la stessa è stata assegnata ad una persona giuridica, deve necessariamente essere un membro della stessa, ossia appartenere alla medesima.*" La Corte ha anche chiarito che quest'ultima espressione è da intendersi come subordinazione, e non invece come conferimento di incarico professionale, che non escluderebbe un certo grado di autonomia nell'espletamento delle mansioni.

3.5

Autoriciclaggio e bancarotta fraudolenta: la pronuncia della Cassazione

Con la sentenza n. 37503 dello scorso 10 settembre la Corte di Cassazione ha sentenziato che la gestione d'impresa può di per sé integrare i presupposti del reato di autoriciclaggio, consentendo anche il sequestro dei beni a carico dell'ente ex artt. 19 e 53 D.Lgs. 231/2001.
Il caso in esame verteva su una vicenda di bancarotta fraudolenta: gli amministratori di una società, precedentemente alla dichiarazione di fallimento, avevano distratto tutte le attività della società tramite contratti di affitto e trasferimento d'azienda fittizi. In relazione a tali condotte delittuose, il GIP di Catania

aveva anche ravvisato i presupposti del reato di autoriciclaggio, poiché gli apicali avevano impiegato "*il complesso aziendale sottratto in modo da occultarne la provenienza delittuosa*". A fronte di ciò, il GIP aveva disposto l'applicazione di misure cautelari nei confronti degli amministratori, nonché il sequestro preventivo di tutti i beni aziendali. Il Tribunale del Riesame, poi, aveva riformato parzialmente l'ordinanza del GIP, stabilendo che il sequestro dei beni aziendali doveva essere limitato all'equivalente del profitto da reato. A fronte di tale pronuncia, i ricorrenti avevano adito la Corte di Cassazione.
Gli Ermellini hanno rigettato il ricorso, confermando il provvedimento disposto dal Tribunale del Riesame, argomentando che la distrazione dell'azienda, se accompagnata dalla successiva gestione della stessa, configura pienamente la fattispecie del reato di autoriciclaggio "*sub specie di impiego in attività economiche ovvero finanziarie dell'utilità di provenienza illecita*".
Il trasferimento d'azienda, quindi, in presenza di un'attività gestoria, può configurare sia il reato di bancarotta fraudolenta (che di per sé non implicherebbe una responsabilità dell'ente ex D.Lgs. 231/2001), che quello di autoriciclaggio.

3.6

Consenso necessario per l'installazione dei cookie. La sentenza della Corte di Giustizia UE

Con la sentenza n. C-673/17 del primo ottobre scorso, la Corte di Giustizia UE (CGUE) ha sancito l'obbligatorietà del consenso attivo degli utenti per l'installazione di cookie sui propri dispositivi, rilevando che le caselle di spunta preselezionate e sovente adottate da diversi siti web per ottenere il consenso degli utenti non equivalgono ad una libera manifestazione dello stesso.
La vicenda prende le mosse da un'azione esperita dalla federazione tedesca delle organizzazioni dei consumatori avverso la società Planet 49 – un operatore di giochi a premi online – con la quale la federazione segnalava l'utilizzo da parte della società di caselle pre-spuntate volte ad ottenere dagli utenti il consenso all'installazione di cookie di natura commerciale.
La decisione della Corte di Lussemburgo ruota intorno al concetto di "*consenso attivo*": nel caso di specie, gli utenti prestavano il proprio consenso passivamente, in quanto l'azione attiva era richiesta non per manifestare il proprio consenso, ma bensì per revocarlo. Così la CGUE: "*il consenso […] non è validamente espresso quando l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet attraverso i cookie sono autorizzati mediante una casella di spunta preselezionata che l'utente deve deselezionare al fine di negare il proprio consenso*"; tutto ciò a prescindere dal fatto che i dati in questione siano personali o meno.

La sentenza in oggetto ha una portata estremamente ampia, potenzialmente in grado di modificare radicalmente l'approccio alla spinosa questione dei cookie, per di più dato che la CGUE ha anche stabilito che i fornitori di servizi online sono tenuti a fornire agli utenti informazioni in merito al periodo di attività dei cookie ed alla possibilità per i terzi di avere accesso agli stessi.

Pirola
Pennuto
Zei
& Associati
studio di consulenza
tributaria e legale

Via Vittor Pisani, 20
20124 Milano

T. +39.02.669951
F. +39.02.6691800

info@studiopirola.com
www.pirolapennutozei.it

COMPLIANCE NEWSLETTER | SETTEMBRE 2019

RIFERIMENTI NORMATIVI, PRASSI E GIURISPRUDENZA AL 30 SETTEMBRE 2019.
LA PRESENTE NEWSLETTER ILLUSTRA 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