NOVEMBRE 2019
WWW.BDO.IT

FLASH
Info Paper

IN QUESTO NUMERO

Cosa

- Decreto Legge n.105/2019, "Perimetro di sicurezza nazionale"
- Legge n.117/2019, 4/10/2019, recepimento della "Direttiva PIF"
- Decreto Legge n.124/2019, decreto fiscale collegato alla Manovra economica 2020

Perimetro

- D. Lgs. 231/2001

Impatti

- Responsabilità penali
- Responsabilità amministrativa della Società ai sensi del D. Lgs. 231/2001
  -> aggiornamento del Modello di Organizzazione, Gestione e Controllo
- Analisi del rischio "fiscale"
  -> adozione del "Tax Control Framework"

contatto: ras@bdo.it
più info: **www.bdo.it**

Compliance
reati fiscali e sicurezza cibernetica: esteso il perimetro della responsabilità ex d.lgs. 231/01

Alla luce delle più recenti novità normative il presente numero del Flash Info Paper si propone di analizzare i possibili impatti ai fini del D.Lgs. 231/2001 sull'aggiornamento dei Modelli di Organizzazione, Gestione e Controllo.

DELITTI CONTRO GLI INTERESSI FINANZIARI DELL'UE

LEGGE DI DELEGAZIONE EUROPEA 2018 -> LOTTA CONTRO LA FRODE CHE LEDE GLI INTERESSI FINANZIARI DELL'UNIONE MEDIANTE IL DIRITTO PENALE

Legge 4/10/2019, n. 117 "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2018"

-> pubblicato in G.U. il 18/10/19 e in vigore dal 2/11/2019

-> recepimento della Direttiva (UE) 2017/1371 (c.d. Direttiva PIF – Protezione interessi finanziari) e introduzione, tra i reati del "catalogo 231" di alcuni reati tributari lesivi degli interessi finanziari dell'UE.

La Legge 4/10/2019, n. 117 all'art. 3 delega il Governo a:

a) individuare i reati previsti dalle norme vigenti che possano essere ritenuti reati che ledono gli interessi finanziari dell'Unione europea, in conformità a quanto previsto dagli articoli 1, 2, 3, 4 e 5 della direttiva (UE) 2017/1371;
[…]

*e) **integrare le disposizioni del decreto legislativo 8 giugno 2001, n. 231,** recante disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, **prevedendo espressamente la responsabilità amministrativa da reato delle persone giuridiche anche per i reati che ledono gli interessi finanziari dell'Unione europea e che non sono già compresi nelle disposizioni del medesimo decreto legislativo;***
[…]

*h) prevedere, ove necessario, che, in caso di reati che ledono gli interessi finanziari dell'Unione Europea, in aggiunta alle **sanzioni amministrative previste dagli articoli da 9 a 23 del decreto legislativo 8 giugno 2001**, n. 231, siano applicabili, per le persone giuridiche, talune delle sanzioni di cui all'articolo 9 della direttiva (UE) 2017/1371 **e che tutte le sanzioni siano effettive, proporzionate e dissuasive**.*
[…]

Il Governo è delegato anzitutto ad individuare, tra i reati fiscali già previsti dalla legislazione italiana, quelli che possono ritenersi lesivi degli interessi finanziari dell'UE.

La Legge di Delegazione Europea, quindi, non impone al Governo di rendere presupposto 231 tutti i reati tributari, ma solo quelli che ledono gli interessi finanziari dell'UE.

È prevedibile che verranno individuati i seguenti reati (quando ledano gli interessi finanziari dell'UE):

- evasione IVA tramite dichiarazione sul valore aggiunto fraudolenta (mediante uso di fatture o di altri documenti per operazioni inesistenti), ex art. 2 D. Lgs. 74/2000;
- evasione IVA tramite dichiarazione sul valore aggiunto fraudolenta (mediante altri artifici), ex art. 3 D. Lgs. 74/2000;
- evasione IVA tramite dichiarazione infedele, ex art. 4 D. Lgs. 74/2000;
- evasione IVA per omessa dichiarazione sul valore aggiunto, ex art. 5 D. Lgs. 74/2000;

nonché

- omesso versamento dell'acconto IVA, ex art. 10 ter D. Lgs. 74/2000.

La stessa Direttiva (UE) 2017/1371 (all'art. 2, comma 2), inoltre, prevede che la condotta illecita, in riferimento alla frode IVA, debba presentare due caratteristiche specifiche (c.d. "reati gravi"):

1) avere una connessione con due o più Stati membri dell'UE;

2) cagionare un danno finanziario complessivo per l'UE di almeno € 10.000.000,00.

Infine, le sanzioni previste per l'ente responsabile del reato saranno sia quelle pecuniarie che quelle interdittive.

Tanto premesso, è da segnalare che quelli sin qui analizzati sono principi direttivi.

I reati fiscali lesivi degli interessi finanziari dell'UE **non sono ancora integralmente presenti nel "catalogo 231"** con l'eccezione di quanto indicato a pag. 5 rispetto alle dichiarazioni fraudolente.

Tale Legge, nondimeno, è indicativa di un'accresciuta sensibilità del Legislatore in materia e della volontà di prevedere, la punibilità, oltre della persona fisica responsabile della condotta illecita, anche dell'ente nel cui interesse o vantaggio sia stato commesso il reato tributario.

DELITTI CONTRO IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

DECRETO-LEGGE N. 105/2019
-> PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Decreto-Legge 21/09/2019, n. 105 "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"

-> pubblicato in G.U. il 21/09/19 e in vigore dal 22/09/2019

-> introduzione, tra i reati del "catalogo 231" dei reati commessi contro il perimetro di sicurezza nazionale cibernetica.

Il Decreto-Legge n. 105/2019 istituisce un **perimetro di sicurezza nazionale cibernetica**, finalizzato ad assicurare un livello elevato 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 l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

A tal fine, l'art. 1 del Decreto stabilisce che:
[…]

2. ***Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto**, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR):*
[…]

*b) **sono definiti i criteri in base ai quali i soggetti di cui alla precedente lettera a) predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica**; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri; entro sei mesi dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al presente comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, individuati ai sensi della lettera a) trasmettono tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico; la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico inoltrano gli elenchi di rispettiva pertinenza al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.*
[…]

*6. Con regolamento, adottato ai sensi dell'articolo 17 comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, **sono disciplinati le procedure, le modalità e i termini con cui**:*

*a) fatti salvi i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni e di servizi ICT cui sia indispensabile procedere in sede estera, **i soggetti di cui al comma 2, lettera a)**, che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), diversi da quelli necessari per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati, ne danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, che, sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità, può, entro trenta giorni, imporre condizioni e test di hardware e software; in tale ipotesi, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, l'affidamento ovvero il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN; per le forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero della difesa, individuati ai sensi del comma 2, lettera b), il predetto Ministero procede, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, in coerenza con quanto previsto dal presente decreto, attraverso un proprio Centro di valutazione in raccordo con la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico per i profili di rispettiva competenza; resta fermo che per lo svolgimento delle attività di*

prevenzione, accertamento e di repressione dei reati e nei casi in cui si deroga all'obbligo di cui alla presente lettera, sono utilizzati reti, sistemi informativi e servizi informatici conformi ai livelli di sicurezza di cui al comma 3, lettera b), qualora non incompatibili con gli specifici impieghi cui essi sono destinati.
[…]

*c) **la Presidenza del Consiglio dei ministri**, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2, lettera a), **e il Ministero dello sviluppo economico**, per i soggetti privati di cui alla medesima lettera, **svolgono attività di ispezione e verifica in relazione a quanto previsto dal comma 2, lettera b), dal comma 3 e dalla lettera a) del presente comma e senza che ciò comporti accesso a dati o metadati personali e amministrativi, impartendo, se necessario**, specifiche prescrizioni; per le reti, i sistemi informativi e i servizi informatici di cui al comma 2, lettera b), connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica sono svolte, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché in tema di prevenzione e di contrasto del crimine informatico, delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti alla Presidenza del Consiglio dei ministri per i profili di competenza.*
[…]

11. Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, 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.
[…]

Viene pertanto previsto un nuovo reato presupposto nel catalogo 231.

Esso consiste nella comunicazione di informazioni non vere che compromettano il perimetro di sicurezza cibernetica ed i controlli sullo stesso.

Più in dettaglio, l'ente sarà responsabile qualora un suo apicale o sottoposto:

- comunichi dati falsi in sede di predisposizione obbligatoria degli elenchi di reti/sistemi/servizi di propria pertinenza rientranti nel "perimetro di sicurezza cibernetica";
- fornisca false comunicazioni al Centro di valutazione e certificazione nazionale (CVCN);
- ostacoli o comunque condizioni le attività ispettive su sistemi informativi e servizi informatici rilevanti per la Pubblica Sicurezza o la Difesa nazionale.

All'ente riconosciuto responsabile di questo reato sarebbe applicata, ai sensi del D. Lgs. 231/01, la sola sanzione amministrativa pecuniaria fino a 400 quote, mentre non sono previste sanzioni interdittive.

Tuttavia, prima essere efficace e vincolante, anche a fini 231, questa nuova normativa dovrà essere:

- convertita in legge;
- integrata dai previsti decreti attuativi che saranno chiamati ad individuare:
- i soggetti destinatari (con decreto del Presidente del Consiglio dei Ministri) della norma;
- gli adempimenti informativi in caso di affidamento di beni/servizi a terzi.

Una volta integrata la normativa, le Società che, in virtù della propria attività strategica o del loro ricorso a beni, strumenti o servizi ICT (Information and Communication Technology), saranno ricomprese nel perimetro di sicurezza cibernetica, dovranno procedere a valutare il rischio di commissione dei reati sopra descritti e ad aggiornare il Modello di Organizzazione e Gestione ex D.Lgs.231/2001.

NUOVO REATO PRESUPPOSTO ART. 25 - QUINQUIESDECIES (REATI TRIBUTARI)

DECRETO-LEGGE N. 124/2019 -> DISPOSIZIONI IN MATERIA FISCALE

Decreto-Legge 26/10/2019, n. 124 "Disposizioni urgenti in materia fiscale e per esigenze indifferibili"

-> pubblicato in G.U. il 26/10/19 e in vigore dal 27/10/2019

-> introduzione dell'art. 25 quinquiesdecies nel D.Lgs. 231/2001

Il Decreto Legge "Disposizioni urgenti in materia fiscale e per esigenze indifferibili" all'art. 39, comma 2, introduce la **dichiarazione fraudolenta** di cui all'art. 2 del D.Lgs. 74/200 tra i reati presupposto ex D.Lgs. 231/2001: "**Art. 25-quinquiesdecies (Reati tributari)** - *In relazione alla commissione del delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2 del decreto legislativo 10 marzo 2000, n. 74, si applica all'ente la sanzione pecuniaria fino a cinquecento quote".*
Il comma 3 dell'art. 39 prescrive che "Le disposizioni di cui ai commi 1 a 2 hanno efficacia dalla data di pubblicazione nella Gazzetta Ufficiale della legge di conversione del presente decreto".
Tale previsione si inserisce nel percorso di inasprimento delle sanzioni applicabili ai reati tributari prevista all'art. 39 del suddetto decreto.

La fattispecie richiamata (art. 2 del D.Lgs. 74/2000) fa riferimento alla condotta di indicare, al fine di evadere le imposte sui redditi o sul valore aggiunto, in una delle dichiarazioni relative a dette imposte, elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti. Il delitto si commette allorquando tali fatture o altri documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

Riprendendo quanto anticipato nella a pag. 2 rispetto alle evasioni IVA, **il Decreto n. 124/2019 apre definitivamente le porte all'introduzione dei reati fiscali tra i reati presupposto ex D.Lgs. 231/2001 rappresentando il primo elemento di "avvicinamento" alla Direttiva PIF.**

Infatti, con la conversione del Decreto, è possibile che la nuova Legge possa portare all'apertura del "catalogo 231" ad altri reati di natura fiscale.

Conseguentemente, è opportuna e auspicabile per le Società l'introduzione di un **sistema di gestione del rischio fiscale e delle relative misure di prevenzione e presidio.**

All'interno del perimetro della compliance ex D. Lgs. 231/2001, le Società dovranno procedere all'aggiornamento del Modello Organizzativo ex D. Lgs. 231/2001, con **una valutazione dei i rischi fiscali connessi alla propria attività** e implementare adeguati protocolli di controllo sui processi che alimentano le dichiarazioni fiscali.

In quest'ottica, il c.d. **"Tax Control Framework", ovvero un sistema di *rilevazione, misurazione, gestione e controllo del rischio fiscale*** può efficacemente **supportare l'aggiornamento delle valutazioni di rischio a fini 231 e la sua adozione può rappresentare un valido strumento di presidio e di controllo delle fonti di rischio fiscale**, ovvero una modalità "ulteriore" e di maggior copertura rispetto alla semplice mappatura del reato in esame nell'ambito del risk assessment 231.

Esso consente:

- di analizzare tutti i processi aziendali con particolare attenzione a quelli di rilevanza fiscale;
- di aderire al regime di adempimento collaborativo con l'Agenzia delle Entrate;
- di implementare un efficiente ed efficace sistema di controllo sui processi aventi rilevanza fiscale,

con conseguente attenuazione del rischio di commissione di reati tributari.

Un tale sistema di controllo può rafforzare sensibilmente l'efficacia del Modello Organizzativo ex D. Lgs. 231/2001 in relazione al rischio di realizzazione di condotte di evasione penalmente rilevanti per i soggetti apicali e riduce la possibilità che all'ente siano erogate sanzioni ai fini 231.

Hanno contribuito alla redazione di questo numero: Stefano Minini, Marco Strafurini, Renato Marro e Giuseppe Carnesecchi

Contatti:

BDO Italia
Viale Abruzzi, 94
20131 Milano
Tel: 02 58 20 10

BDO è tra le principali organizzazioni internazionali di revisione e consulenza aziendale con circa 80.000 professionisti altamente qualificati in più di 160 paesi. In Italia BDO è presente con circa 800 professionisti e 18 uffici, una struttura integrata e capillare che garantisce la copertura del territorio nazionale.

La redazione di questo numero è stata completata il 6 novembre 2019.

Audit | Advisory | Outsourcing | Tax | Law

www.bdo.it