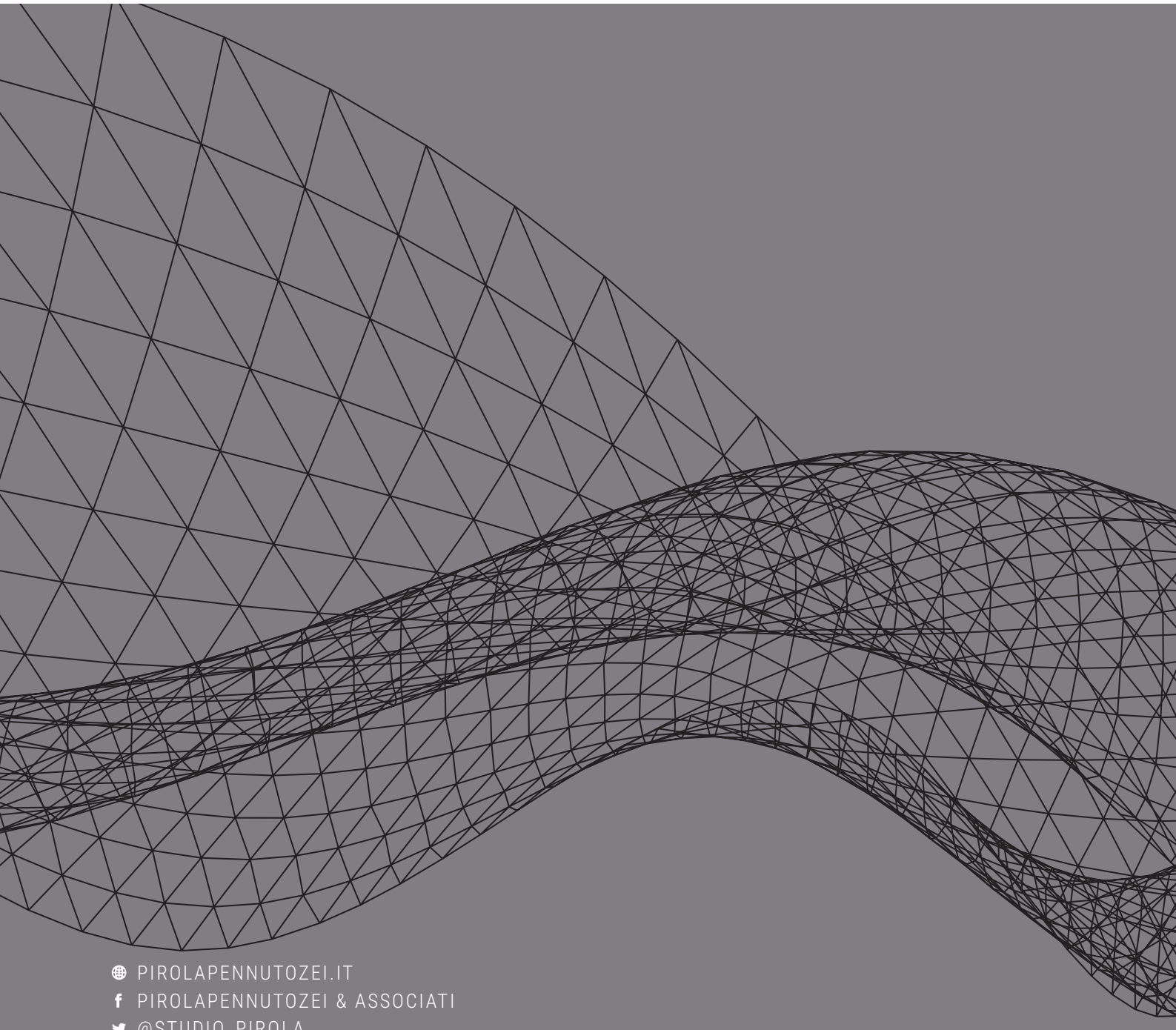
Pirola
Pennuto
Zei
& Associati

studio di consulenza
tributaria e legale

COMPLIANCE

NEWSLETTER / SEPTEMBER 2019



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

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDEX

LEGISLATION

GUIDANCE

CASE LAW

BACK TO TABLE OF CONTENTS ↑

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDEX

LEGISLATION

1.1

Germany moves one step forward in corporate criminal liability legislation

The German Justice Ministry has recently published a bill on corporate criminal liability, broadly similar to Italian legislative decree 231/2001, introducing a penalty system for companies in connection with crimes committed by their managers, as well as incentives for the conduct of internal audits, and thoroughly revising search and seizure legislation.
As is already the case under Italian legislation, the bill provides for a substantial reduction of penalties if companies implement an adequate compliance program.
The new legislation introduced significant pecuniary penalties, as high as 10% of the average annual sales of the three fiscal years prior to the commission of the crime for companies with an annual turnover of €100 million.
The new rules also apply to crimes which, albeit committed outside the German territory, can be connected to a German-based company.

1.2

The new decree law on national cybersecurity, introducing a new predicate offence, has entered into force

Decree Law No 105 of 21 September 2019, containing urgent provisions on national cybersecurity and introducing a new predicate offence for the purposes of corporate liability under legislative decree 231/2001, was published on 22 September.
The Decree was issued in the wake of the concerns raised about the creation of the 5G infrastructure in Italy and intends to ensure a high level of security of the IT networks, systems and services of the public authorities and the national public and private entities, on which rely fundamental functions of the State and whose malfunction, interruption or improper use could raise national security issues; the technical requirements, the persons involved and the manner of application will be established in subsequent enactments.
The decree introduces a new case relevant for the purposes of decree 231/2001: anyone who – with a view to hindering or conditioning the performance of obligations concerning 1) the preparation and update, at

least on an annual basis, of network lists, IT systems and IT services, 2) procedures for the contracting out of such ICT services, or 3) inspections and audits on the compliance with the decree by the competent authority – provides false data, information or factual elements necessary for the performance of such obligations, or fails to provide them within the legally prescribed term, "*shall be punished by imprisonment between one and five years and the entity liable pursuant to legislative decree 231/2001 shall be subject to a fine of up to four hundred quotas*".

1.3

The Italian chamber of deputies approved the legislation on corporate liability for VAT fraud

On 1 October, the Italian Chamber of Deputies definitively approved the 2018 European delegation law, delegating *inter alia* "*Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law" (the "PIF Directive*").

The Directive introduced corporate liability for serious offences against the common VAT system, i.e., offences that are connected "*with the territory of two or more Member States and the total damage caused by the offences is at least EUR 10,000,00*".

The Parliament delegated the government to identify the offences against the EU's financial interests, the relevant penalties, the abrogation of any incompatible rules and the additions to be made to legislative decree 231/2001.
The Directive specifies, by way of example, a number of appropriate penalties for legal persons, such as for instance "*the temporary or permanent exclusion from public tender procedures, the temporary or permanent disqualification from the practice of commercial activities and the temporary or permanent closure of establishments which have been used for committing the criminal offence*"(article 9), in addition to the freezing and confiscation of instrumentalities and proceeds from the criminal offences (article 10).
The Government shall issue the relevant legislative measures within three months from the date of the entry into force of the 2018 European delegation law.

GUIDANCE

2.1

The Italian Data Protection Authority has approved the new code of conduct of credit information systems

By Enactment No 9141941 of 12 September, the Italian Data Protection Authority approved the new "*Code of conduct for information systems managed by private entities regarding consumer credit, reliability and punctuality in payments*", incorporating the changes introduced by the GDPR.

The new Code of conduct is focused on strategic areas such as mortgage loans, borrowings, rentals, finance leases, FinTech loans; the Authority declared that to ensure the proper functioning of the financial and credit market, the data gathered may be processed without the data subjects' consent, on the basis of the legitimate interest of the credit information companies, while at the same time ensuring the broadest rights under the general data protection regulation.

In this context, the Code lays the emphasis on the data minimization principle pursuant to article 5 of the GDPR, according to which personal data must be adequate, relevant and limited to the specific purpose of processing – in this case, credit risk assessment.

Further there is an obligation for the companies managing credit information systems to periodically update – at least every two years – the statistical analysis models and the algorithms used.

CASE LAW

3.1

Morele.net has been fined EUR 660,000 for breaching the principle of integrity and confidentiality of personal data

On 19 September, the Polish data protection authority ("*UODO*") inflicted a EUR 660,000 fine on Morele.net, an online retailer, for a breach of its customer data occurred in December 2018. This is so far the highest penalty for a breach of personal data protection rules.
The data breach resulted in the theft through phishing of the names, email addresses, postal addresses and telephone numbers of about 2.2 million users.
The company notified the Authorities and the data subjects concerned of the data breach within the time required by the GDPR, but the subsequent investigation showed that the technical and organizational measures adopted by Morele.net were inadequate as, apparently, the online retailer failed to observe the principle of integrity and confidentiality, referred to in article 5(1)(f) of the GDPR, pursuant to which personal data are to "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*".
UODO also accused Morele.net of performing the inadequate monitoring of potential threats to personal data, as it failed to react with sufficient promptness when it realized that personal data were being massively downloaded.

3.2

Italian anti-corruption authority (ANAC): infliction of the first penalty for violation of the prohibition to retaliate against a whistleblower

During their meeting of 4 September, the Italian national anti-corruption authority issued – by resolution No 782 - its first penalty for the violation of the prohibition to retaliate against a whistleblower.
The dispute concerned a report filed by a senior officer of a municipality in Campania against employees of the municipality's Office of Disciplinary Proceedings - who had dismissed disciplinary proceedings for verbal abuse suffered by such senior manager - for abuse of office and failure to carry out their duties.

The whistleblower had subsequently been suspended from work without pay and was accused of violating

the Municipality's code of conduct according to which any illegal conduct had to be first confidentially reported to the corruption-prevention manager.
During the disciplinary proceedings, the whistleblower had been denied the protection provided by article 54-*bis* of legislative decree 165/2001 ("*Protection of a public officer reporting illegal conduct*"), on the grounds that anonymity was considered essential to qualify as a whistleblower.
On this complex issue, the Italian anticorruption authority issued a statement to the effect, *inter alia,* that the whistleblower need not remain anonymous and that his obligation to report the facts pursuant to the Italian Penal Code and the Code of Criminal Procedure did not affect his status as whistleblower (considering the broader scope of article 54-*bis* of legislative decree 165/2001).

3.3

European Court of Justice: the right to be forgotten does not extend beyond the EU

In its 24 September ruling on case C-507/17, the ECJ stated that the right to be forgotten only applies to the EU territory, whereas personal data may continue to be available outside it.
The case resulted from proceedings between the "*Commission Nationale de l'Informatique et des Libertés*" ("*CNIL*") – the French Privacy Authority – and Google, concerning a penalty of EUR 100,000 imposed by the CNIL on Google because of that company's refusal, when granting a de-referencing request, to apply it to all its search engine's domain name extensions. Google sought annulment of the Authority's adjudication by application lodged with the *Conseil d'État* (French Council of State). The "*Conseil d'État*", then filed a request for a preliminary ruling with the ECJ on whether a search engine operator is required to carry out de-referencing on all versions of its search engine – including its non-EU versions - or whether, on the contrary, it is required to do so only on the versions of that search engine corresponding to all the Member States.

The ECJ noted that the right to be forgotten is not granted outside the EU and that the right to the protection of personal data is not an absolute right but must be considered in relation to its function in society and be balanced against other fundamental rights, and concluded by saying that under European legislation the right to be forgotten must not be applied to all versions of its search engine but only to its EU versions.

3.4

Administrative Court of Apulia: if the DPO is a legal person, the individual in charge must be one of its employees

The Administrative Court of Apulia in Lecce has recently pronounced on the matter of the DPO (*Data Protection Officer*) in decision No 1468/2019 – published on 13 September – specifying that, where the Data Controller or the Data Processor appoint a company as DPO, the individual who will actually carry out the relevant duties must necessarily be an employee of such company.

The case focused on an appeal against the ranking of tenders called by the Municipality of Taranto for the appointment of a DPO: the first ranking company had identified an independent contractor as the individual in charge of covering the position of DPO.

The Court, basing its decision on the "*Linee guida sui responsabili della protezione dei dati*" (Guidelines concerning DPOs) of 13 December 2016, ruled that, when the role of DPO has been assigned to a legal person, the individual holding the actual office must be a member of the organization, meaning an employee of such legal person, and not an independent contractor, which would be able to carry out his/her duties with a certain degree of independence.

3.5

The Italian Supreme Court rules on self-laundering (***Autoriciclaggio***) and fraudulent bankruptcy (***Bancarotta fraudolenta***)

In its decision No 37503 of 10 September, the Italian Supreme Court ruled that business management activities can satisfy the conditions for the offence of *autoriciclaggio* (self-laundering), with the consequent possibility that the company's assets may be seized pursuant to articles 19 and 53 of legislative decree 231/2001.

The decision concerned a case of fraudulent bankruptcy: before the bankruptcy ruling, the directors of a company had diverted all of the company's assets through a fake transfer of business and fictitious rental agreements. In this connection, the Catania judge for preliminary investigations (*giudice per le indagini preliminari* – GIP) had identified the conditions for the offence of *autoriciclaggio*, since the company's managers had used the business thus diverted in such a way as to conceal its illegal provenance and for this reason had ordered precautionary measures against the directors and the precautionary attachment of all corporate assets. The Italian *Tribunale del Riesame* (a court of review) had partially amended the judge's order, establishing that only the corporate assets of a value corresponding to the illicit gain had to

be seized. The managers had appealed against this decision to the Italian Supreme Court, which however rejected the appeal and confirmed the court of review's decision, on the grounds that illegally diverting a business and subsequently managing it constitutes a case of *autoriciclaggio* (use of illicit gains in business or financial activities).
Therefore the illegal transfer and subsequent management of a business may give rise to both fraudulent bankruptcy (which would not per se trigger corporate liability pursuant to legislative decree 231/2001) and *autoriciclaggio.*

3.6

ECJ ruling: the installation of cookies requires consent

In its decision on case C-673/17 dated 1 October, the ECJ stated that users' active consent was required in order to install cookies on their devices and that to this effect acceptance of the pre-ticked checkboxes adopted by different websites to obtain such consent did not constitute an indication of a user's wishes.
The decision was the result of action taken by the German Federation of Consumer Organisations, against Planet 49 – an online gaming company – which the Federation claimed used pre-checked boxes to obtain users' consent to the installation of advertising cookies.
The ECJ ruling is based on the notion of "*active consent*": in this specific case, users gave their passive consent, while an active behavior was required only to revoke their consent to the installation of cookies.
In the ECJ's words "*the consent […] is therefore not validly constituted if the storage of information, or access to information already stored in an website user's terminal equipment, is permitted by way of a checkbox pre-ticked by the service provider which the user must deselect to refuse his or her consent*"; this applies to personal data and other data alike.
The decision has an extremely broad scope and may radically amend the approach to the thorny issue of cookies, all the more so since the ECJ also stated that online service providers are required to provide users with information on the duration of the operation of the cookies and whether or not third parties may have access to those cookies.

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 | SEPTEMBER 2019

LEGISLATION, MINISTERIAL GUIDANCE AND CASE LAW AT 30 SEPTEMBER 2019.
THIS NEWSLETTER IS INTENDED AS A SUMMARY OF KEY DEVELOPMENTS AND HIGHLIGHTS MATTERS OF GENERAL INTEREST, AND THEREFORE SHOULD NOT BE USED AS A BASIS FOR DECISION-MAKING.
FOR FURTHER DETAILS AND INFORMATION, PLEASE CONTACT YOUR RELATED PARTNER OR SEND AN EMAIL TO UFFICIOSTUDI@STUDIOPIROLA.COM