

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 per la Qualità, la Sicurezza negli ambienti di lavoro, la Privacy, l'Ambiente, l'Etica, per i Modelli Organizzativi e Consulenza per la Direzione

2023 Dicembre *Il nostro punto di vista su...* Anno 16 – 2° sem



**Periodico di informazione
per i CLIENTI dello STUDIO VIOLI**

Indice delle NOTIZIE (N)



- **N1) D.Lgs. 231/01:** Whistleblowing - scadenza il 17 dicembre 2023 per le aziende con dipendenti tra 50 e 249 e per le aziende con meno di 50 dipendenti ma che abbiano adottato il MOG 231. Servizi dello Studio Violi
- **N2) Privacy:** Il furto dei dati è da risarcire
- **N3) Privacy: Videosorveglianza:** Il Garante della Privacy censura l'ente pubblico che impiegava ancora i vecchi modelli di cartelli
- **N4) Privacy:** prove e simulazioni in caso di richiesta di documenti privacy da parte delle autorità
- **N5) Sicurezza:** Riduzione Premio INAIL 2024: sconti e novità del modello OT23
- **N6) Ambiente:** RENTRI pubblicato il Decreto Direttoriale che definisce le modalità operative
- **N7) Responsabilità ESG:** Environmental, Social, and Governance

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

“L'informazione è la fonte dell'apprendimento ma, a meno che non sia organizzata, elaborata e resa disponibile alle persone giuste in un formato per prendere decisioni, è un peso, non un beneficio”

William Pollard – biografo inglese

Scadenziario di Dicembre 2023 sul sito del Sole 24 Ore <http://www.ilssole24ore.com/norme-e-tributi/scadenze.shtml>



E-mail: info@studiovioli.com SDI: giorgiovioli@pec.it
Web: www.studiovioli.com Fax: 059 682304

Studio Violi Srl - Via per Capanna Tassone, 1156 41021 Ospitale - Fanano (MO)
P.I. e C.F. 02836380366 – REA 335410 CCIAA MO – Cap. Soc. € 10.000 I.V.



“Sistema di fissaggio: dov’è l’errore?” *risposta a fine pagina

* spostando i sacchi la piattaforma cade *

Notizie



- N1) D.Lgs. 231/01: Whistleblowing - scadenza il 17 dicembre 2023 per le aziende con dipendenti tra 50 e 249 e per le aziende con meno di 50 dipendenti ma che abbiano adottato il MOG 231. Servizi dello Studio Violi

In questi mesi sono stati approfonditi e dibattuti i temi della applicazione concreta in azienda di questi obblighi di legge, stante gli adempimenti previsti nei vari campi (principalmente 231 e privacy), con previsioni di vari pareri e soluzioni, considerata l'attuale mancanza di giurisprudenza su questi temi.

Le attività di adeguamento devono essere completate entro il 17 dicembre aggiornando il set di documenti (principalmente 231 e privacy) a cura dei rispettivi consulenti aziendali a supporto della piattaforma scelta.

Gli adempimenti puntuali proposti con uno specifico servizio dello studio Violi, sono i seguenti:

1. Definire la politica per la gestione delle segnalazioni
2. Definire i canali di comunicazione (interni o esterni), compresa la piattaforma software
3. Effettuare la DPIA del canale informatico
4. Aggiornare il Registro dei trattamenti
5. Definire la procedura per l'effettuazione e la gestione delle segnalazioni
6. Comunicazione ai Sindacati interni
7. Predisporre l'informativa per chi segnala compresi i Dipendenti e Collaboratori
8. Autorizzare al trattamento dei dati della segnalazione
9. Formare il personale autorizzato al trattamento
10. Stipulare i contratti con i Responsabili
11. Informare sul sistema di segnalazioni adottato
12. Aggiornare il Modello di prevenzione reati (MOG)
13. Aggiornare il codice etico
14. Aggiornare il sistema disciplinare

Per quanto riguarda la "piattaforma software" (punto 2 degli adempimenti e ultima grande novità) sul mercato locale sono presenti alcune piattaforme commerciali (oltre al software open gratuito "Global leaks" che però è da configurare specificatamente).

In officina di fornire un servizio completo ai propri Clienti, Studio Violi Srl ha stipulato una partnership con la società "XDataneet Srl".

Le specifiche della piattaforma sono disponibili a richiesta.

Per quanto riguarda la fornitura dei modelli di cui ai punti precedenti sugli adempimenti obbligatori (1-14) e la consulenza per il corretto adeguamento agli adempimenti necessari collegati alla piattaforma di comunicazione di coloro che segnalano abusi e alla gestione del Whistleblowing (WB) in azienda con tutte le azioni relative, lo Studio Violi Srl ha predisposto uno specifico progetto "ad hoc".

L'ANAC applica una sanzione da 10.000 euro a 50.000 euro, in particolare laddove accerta che:

- **non sono stati istituiti canali di segnalazione o non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero l'adozione o la loro implementazione non è conforme alla normativa.**

- N2) Privacy: Il furto dei dati è da risarcire

Strada spalancata al risarcimento dei danni in caso di data breach. Gli interessati possono chiedere i danni immateriali all'impresa che ha subito un cyberattacco con esfiltrazione dei dati personali, anche se i dati non sono stati ancora usati da delinquenti

Gli interessati possono chiedere i danni immateriali all'impresa che ha subito un cyberattacco con esfiltrazione dei dati personali, anche se i dati non sono stati ancora usati da delinquenti.

A sostenere che, per avanzare una richiesta risarcitoria, non c'è bisogno di aspettare un effettivo furto dell'identità (bastando il furto dei dati) è l'avvocato generale della Corte di Giustizia Ue (Cgue), che nelle sue conclusioni del 26/10/2023 relative alle cause riunite C182/22 e C189/22 ha chiesto alla Cgue un'interpretazione del Gdpr (regolamento Ue sulla privacy) molto favorevole agli interessati.

Nella vicenda che ha dato origine alla controversia, due investitori hanno aperto depositi titoli presso un'applicazione di trading on line gestita da una società. Al fine di verificare la loro identità, gli utenti hanno dovuto registrare i dati personali nell'applicazione, fra i quali nome, data di nascita, indirizzo fisico e di posta elettronica e anche una copia digitale delle carte d'identità. La piattaforma ha subito un attacco informatico e soggetti ignoti, autori del reato, hanno rubato i dati degli utenti. Gli investitori hanno fatto causa alla società di trading, chiedendo il risarcimento del danno immateriale per il dolore e la sofferenza patito a causa dell'esfiltrazione dei dati, conservati nell'applicazione di trading. Non risulta che i ladri digitali abbiano utilizzato i dati.

Il tribunale, chiamato a decidere la controversia, ha chiesto alla Cgue l'esatta interpretazione di alcune norme del Gdpr, rilevanti nel caso concreto. In particolare, il giudice della controversia principale ha chiesto se per avere diritto al risarcimento dei danni immateriali, l'autore dell'illecito deve avere usato effettivamente i dati sottratti o, invece, se il furto risarcibile si verifichi già solo per effetto della disponibilità, da parte degli autori del reato, di dati che rendono identificabile l'interessato. In effetti, alcune premesse al Gdpr (chiamati "considerando") citano espressamente solo il furto di identità ed è comprensibile il dubbio sollevato dal giudice del merito della causa. Al riguardo, le conclusioni distinguono il furto di dati dal furto di identità: solo il secondo tipo di furto implica l'effettivo utilizzo delle informazioni sottratte. **Peraltro, anche se non costituisce un furto o un'usurpazione d'identità, il mero furto di dati personali può comportare un danno immateriale e un diritto al risarcimento dei relativi danni. Questa impostazione, se confermata dalla Corte Ue, amplierà la possibilità di chiedere il risarcimento a tutti i casi in cui un'impresa subisca un data breach con esfiltrazione dati, anche se non risulti un effettivo utilizzo dei dati rubati.**

- N3) Privacy: Videosorveglianza: Il Garante della Privacy censura l'ente pubblico che impiegava ancora i vecchi modelli di cartelli

Il titolare del trattamento è tenuto a rispettare i principi in materia di protezione dei dati, fra i quali quello di "liceità, correttezza e trasparenza" nonché di "minimizzazione", in base ai quali i dati personali devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" e devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. a) e c), del GDPR.

Il principio di "liceità, correttezza e trasparenza" (art. 5, par. 1, lett. a del Regolamento europeo), consiste nel dovere del trattamento di adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli

artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (v. art. 12 GDPR).

Nel corso di un recente provvedimento (Prov. 9 giugno 2022 [Doc. Web 9794895]) l'Autorità Garante per la protezione dei dati personali ha censurato un Comune che utilizzava i modelli di segnaletica non aggiornati alle Linee Guida EDPB n.3/2019 sui trattamenti di dati attraverso strumenti video.

In base ai nuovi modelli, oltre a rendere l'informativa di primo livello, mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, il Titolare deve fornire agli interessati anche delle "informazioni di secondo livello", che devono "contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]" ed "essere facilmente accessibili per l'interessato".

Sul punto si veda il § 7 delle "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", il § 3.1. "Provvedimento in materia di videosorveglianza" del Garante dell'8 aprile 2010 e infine, la FAQ n. 4 del Garante in materia di videosorveglianza, doc. web 9496574.

Nel caso affrontato dal Garante nei confronti di un Comune si legge: "Al riguardo, si osserva che risulta, tuttavia, errato – in quanto non più attuale - il richiamo, effettuato nel cartello utilizzato dal Comune [OMISSIS] all'art. 13 del Codice, che è stato abrogato dal d.lgs. 10 agosto 2018, n. 101. Inoltre, tale cartello, che è, peraltro, sprovvisto di riferimenti ai diritti degli interessati, non indica le modalità con le quali gli interessati [OMISSIS] possono ricevere un'informativa completa sul trattamento di secondo livello. Né emerge dagli atti che il Comune abbia provveduto a redigere tale informativa di secondo livello e portarla a conoscenza degli interessati, ad esempio mediante pubblicazione della stessa sul sito web istituzionale del Comune."

Ricordiamo in conclusione che le informazioni dovrebbero essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi) "per consentire all'interessato di stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario". (in questo senso Prov. 15 Settembre 2022 – doc. web. N. 9815745).

-N4) Privacy: prove e simulazioni in caso di richiesta di documenti privacy da parte delle autorità

La prima cosa che il Nucleo Speciale della Guardia di Finanza chiede quando fa una visita ispettiva è il registro dei trattamenti. È una richiesta che fa sia quando controlla il titolare del trattamento che il responsabile esterno. E non accetta ritardi!

Il registro dei trattamenti è alla base del principio di accountability, che vuol dire responsabilità piena e rendicontazione obbligatoria. Perché il titolare deve essere in grado di dimostrare e di documentare di aver fatto il trattamento in conformità del Regolamento. E lo fa attraverso il registro. Una volta c'erano le misure minime di sicurezza. Ma oggi non è più così: ogni titolare deve implementare delle misure adeguate ed è sua la responsabilità.

Le informazioni minime da inserire nel registro sono:

- Le finalità del trattamento, cioè il motivo per cui raccogli i dati personali. Per fare pubblicità? Per fare altro? Per cosa?
- Le categorie di dati trattati (dati personali comuni, particolari, di credito e così via).
- Le categorie di interessati, cioè delle persone fisiche: sono dipendenti, clienti, prospect?
- I tempi di conservazione: per quanto tempo tratti quei dati?
- Le misure di sicurezza: quali soluzioni fisiche, tecnologiche ed organizzative hai adottato per garantire la protezione dei dati? Esempio. Oggi tutti accedono a tutto: non va bene. Perché poi può succedere quello che accaduto di recente con la TIM - un caso che è uscito su tutti i giornali - in cui si è scoperto che alcuni dipendenti infedeli sono entrati nel database con le loro password e hanno scaricato centinaia di migliaia di dati personali dei clienti per rivenderli ad altre società. Se mi occupo dei clienti, devo

accedere solo ai dati dei clienti. Se mi occupo dei fornitori, devo accedere solo ai dati dei fornitori. Se mi occupo di geolocalizzazione, accedo solo a quei dati. Ai dati dei dipendenti devono accedere solo i dipendenti dell'HR. Ognuno accede ai dati che gli servono per la sua attività lavorativa. E la Guardia di Finanza ci guarda!

- I trasferimenti: i destinatari (persone fisiche o giuridiche) a cui saranno comunicati i dati e il Paese di destinazione. Devi sapere a chi hai comunicato i dati di Peppino, Antonio e Giulia.
- I dati di DPO e Cotitolari

Registro, informativa, sistemi informatici: tutto deve essere allineato

Il registro dei trattamenti deve essere aggiornato, altrimenti non è adeguato

Può essere cartaceo o in digitale, l'importante è che sia immediatamente consultabile

Fonte: Giuseppe Giuliano

- N5) Sicurezza: Riduzione Premio INAIL 2024: sconti e novità del modello OT23

Riduzione premi INAIL per interventi di prevenzione: nuovo modello OT23, istruzioni di compilazione e scadenza per le domande

L'INAIL ha aggiornato il modello OT23 per la riduzione dei premi assicurativi, godendo cioè di uno sconto sulla tariffa legato alla prevenzione (interventi per il miglioramento delle condizioni di salute e sicurezza nei luoghi di lavoro).

Nella nuova versione, è stato corretto un refuso contenuto nell'intervento B1 (erogazione del corso teorico-pratico di guida sicura), ora riferito ai "lavoratori che durante l'attività lavorativa fanno uso di veicoli a motore personalmente condotti, uno specifico corso teorico-pratico di guida sicura".

Il modello va presentato entro il 29 febbraio 2024 in sede di autoliquidazione 2023/2024.

Il modello OT23 deve essere presentato esclusivamente tramite il servizio online dell'INAIL ed entro febbraio da parte delle imprese che intendano ottenere la riduzione del tasso medio di tariffa.

Come sempre, al modulo deve essere allegata anche la documentazione che attesti gli interventi effettuati. La domanda può essere presentata a prescindere dall'anzianità dell'attività assicurata nella posizione assicurativa territoriale (PAT) ma gli interventi di miglioramento devono essere stati realizzati nell'anno precedente a quello della presentazione.

Lo sconto dal 5 al 28% vede nei primi due anni di attività la riduzione fissa all'8%.

Nel Modello OT23 vanno riportati gli interventi per il miglioramento delle condizioni di salute e sicurezza nei luoghi di lavoro, in aggiunta a quelli previsti dalla normativa in materia effettuati per raggiungere il punteggio minimo che danno diritto alla riduzione dei premi INAIL.

Ogni intervento ha un punteggio: per avere accesso alla riduzione viene richiesto il raggiungimento di almeno 100 punti.

Le novità del Modello di Domanda

- Riformulata la descrizione e la documentazione per gli interventi A-3-2, A-3.4 e A-3.5.
- Ampliato l'intervento A-3.6.
- Riformulato l'elenco dei documenti per l'intervento A-5.1.
- Ridotta la documentazione per l'intervento B-10.
- Esplicitato il riferimento alla norma UNI 11347 per l'intervento C-1.2.
- Eliminato l'intervento C-2.1 sul controllo dei DPI.
- Aggiornato l'intervento C-2.2.
- Esplicitata la tempistica relativa al punto D-3.
- Integrato l'intervento E-3.
- Ampliato l'elenco dei sistemi di gestione previsti al punto E-4.
- Riformulato e aggiornato l'intervento E-5.
- Eliminati gli interventi E-9 ed E-14.
- Inserite precisazioni nell'intervento E-17.
- Nuovi documenti per l'intervento F-2.
- Ampliato l'intervento F-7.

Il link per il modello: https://www.inail.it/cs/internet/docs/alg-modello-ot23-2024_6443196992485.pdf

- N6) Ambiente: RENTRI pubblicato il Decreto Direttoriale che definisce le modalità operative

Il Decreto Direttoriale è completato da istruzioni, presentate in 18 schede, per l'accesso e l'iscrizione al RENTRI da parte degli operatori e loro delegati, i requisiti informatici richiesti per garantire l'interoperabilità del RENTRI con i sistemi gestionali adottati dagli operatori, gli strumenti di supporto a disposizione.

Con la pubblicazione del Decreto Direttoriale MASE del 6 novembre 2023 n. 143 sul sito istituzionale del Ministero dell'ambiente e della sicurezza energetica www.mase.gov.it e sul sito web del RENTRI www.rentri.gov.it sono state approvate le modalità operative per la trasmissione dei dati al RENTRI (Registro Elettronico Nazionale per la Tracciabilità dei Rifiuti), come previsto dall'articolo 21, comma 1, lettere a), b), c) e g) del Decreto del Ministero dell'Ambiente e della Sicurezza Energetica del 4 aprile 2023, n. 59.

Si prevede che con successivi Decreti Direttoriali verranno approvate le modalità di compilazione dei modelli allegati al D.M. 4 aprile 2023, n. 59, Formulario di Identificazione Rifiuto (FIR) e Registro di carico e scarico, i requisiti per i servizi di consultazione da parte delle amministrazioni interessate, i manuali e le guide sintetiche a supporto degli operatori e degli utenti.

Attivato dall'8 novembre 2023 il portale del RENTRI al link www.rentri.gov.it

- N7) Responsabilità ESG: Environmental, Social, and Governance

ESG è un acronimo che sta per "Environmental, Social, and Governance," il quale rappresenta tre categorie di fattori che vengono utilizzate per valutare le prestazioni e la sostenibilità di un'azienda o di un investimento. Ecco cosa rappresentano questi tre componenti:

1. Ambientale (Environmental)

Si riferisce ai fattori legati all'ambiente e alla sostenibilità. Include questioni come l'impatto ambientale di un'azienda sul pianeta, le sue politiche di gestione delle risorse naturali, la riduzione delle emissioni di gas serra, l'efficienza energetica e altre preoccupazioni ambientali.

2. Sociale (Social)

Riguarda i fattori legati alla responsabilità sociale dell'azienda. Include temi come la diversità e l'inclusione nei luoghi di lavoro, la responsabilità sociale d'impresa, i diritti dei lavoratori, la sicurezza sul lavoro, la relazione con le comunità locali e la gestione delle catene di approvvigionamento.

3. Governance

Si riferisce alla governance aziendale e alla struttura di gestione dell'azienda. Include elementi come la composizione del Consiglio di Amministrazione, la trasparenza delle operazioni aziendali, le politiche di remunerazione dei dirigenti, la gestione dei conflitti di interesse e la qualità della supervisione aziendale.

La valutazione ESG è diventata sempre più importante negli investimenti e nelle decisioni aziendali poiché riflette una visione più ampia della sostenibilità aziendale, tenendo conto non solo degli aspetti finanziari ma anche degli impatti ambientali e sociali delle attività aziendali, così come dell'efficacia della loro governance. Gli investitori, le aziende e gli stakeholder stanno sempre più prendendo in considerazione questi fattori nella loro valutazione delle opportunità e dei rischi.

SINTESI DELLE SCADENZE

1. **Whistleblowing:** entro 17 dicembre 2023
2. **Ispezioni garante privacy (estratto):** entro fine 2023
 - a. corretta implementazione delle Linee guida sui cookie e gli altri strumenti di tracciamento;
 - b. osservanza delle disposizioni in materia di protezione dei dati personali, ivi incluse le istruttorie relative a reclami e segnalazioni formali proposti all'Autorità
3. **Qualifica del tecnico manutentore antincendio:** settembre 2024
4. **Bilancio di sostenibilità:**
 - a. società già soggette alla direttiva sulla dichiarazione non finanziaria - NFRD: esercizio 2024, con prima dichiarazione di sostenibilità pubblicata nel 2025;
 - b. altre grandi imprese: esercizio 2025, con prima dichiarazione di sostenibilità pubblicata nel 2026;
 - c. PMI quotate: esercizio 2026, con le prime dichiarazioni di sostenibilità pubblicate nel 2027;

Voglia gradire i nostri più cordiali saluti

ing. Giorgio Violi ing. Alberto Sant'Unione

PregandoLa di scusarci per il disturbo eventualmente arrecato, Le comuniciamo che i Suoi dati sono registrati nel Database Studio Violi srl e questo messaggio Le è stato inviato confidando che i temi trattati potessero essere di Suo interesse. In ottemperanza al Reg. 679/2016/UE, qualora non desiderasse più ricevere questo mensile dallo Studio Violi srl (titolare del trattamento dei dati), può comunicarcelo via mail all'indirizzo info@studiovioli.com. Garantiamo in ogni momento il rispetto di tutti i diritti di cui al Reg. 679/2016/UE.
Credits: si ringraziano le società che hanno facilitato la stesura del presente con la fornitura di parte del materiale, in particolare garante privacy, punto sicuro, ats, ipsoa, il sole24ore, tuttoambiente, iae, quotidiano sicurezza.it, privacylawconsulting, la repubblica, italia oggi, epc, postilla, necsi. Può inoltre contare sulla ns disponibilità ad approfondire i temi qui trattati