

Pisa, 25 maggio 2023

PLS LEGAL S.R.L.
SOCIETÀ TRA AVVOCATI

GLI IMPATTI PRIVACY NEI MODELLI ORGANIZZATIVI E NELLE VERIFICHE DELL'ORGANISMO DI VIGILANZA

PLS LEGAL | VIA FILIPPO TURATI, 26 – 20121 MILANO | VIA CORSICA, 10 – 25125 BRESCIA | legal@plslegal.eu | WWW.PLSLEGAL.EU



ELEMENTI ESSENZIALI DELL'IMPIANTO 231/01

- Il **Decreto Legislativo 231/2001** introduce un regime di responsabilità amministrativa, per le persone giuridiche e le associazioni non riconosciute.
- Per andare esente da tale responsabilità la persona giuridica dovrà:
 1. Implementare ed efficacemente attuare un **Modello Organizzativo (MOG)**, che:
 - a) individui le attività sensibili alla commissione di potenziali reati;
 - b) preveda specifici protocolli per la prevenzione dei reati presupposto;
 - c) stabilisca le procedure per gestire le risorse per la prevenzione di tali reati;
 - d) indichi gli obblighi di comunicazione all'Organismo di Vigilanza;
 - e) Introduca un sistema disciplinare;
 - f) preveda sistemi che permettano e tutelino l'invio di segnalazioni in via riservata.
 2. Nominare un **Organismo di Vigilanza** che vigili e controlli sul rispetto del MOG.
 3. Adottare un **Codice Etico**.

LA PRIVACY NEL SISTEMA 231 (I)

- **Qualificazione dell'Organismo di Vigilanza:** Autorizzati (o autorizzato, qualora l'OdV sia monocratico) al trattamento, senza distinzione tra membri interni e membri esterni (cf. *«Parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231»*);
- **Qualificazione delle attività:** le attività di vigilanza e controllo ex art. 6 co. 1 lett. b) e d) d.lgs.231/2001 poste in essere dall'OdV comportano il trattamento anche di dati personali, sia comuni che particolari (ex art. 9 par. 1 del GDPR).

LA PRIVACY NEL SISTEMA 231 (I)

- **Adempiere agli obblighi di:** **1)** misure di sicurezza tecniche ed organizzative (art. 32 del GDPR), **2)** indicare tali trattamenti nel registro delle attività da titolare del trattamento (ex art. 30 par. 1 del GDPR); **3)** informativa per gli interessati (artt. 13 e 14 del GDPR), **4)** istruzioni operative per il trattamento dei dati per i membri dell'OdV (ex artt. 29 del GDPR e 2 quaterdecies del Codice della Privacy);
- **Si consiglia inoltre di:** eseguire una valutazione sulla necessità di effettuare una valutazione d'impatto e, se necessario, procedere con tale valutazione d'impatto (art. 35 del GDPR).

231/01 E SISTEMI PRIVACY: ANALOGIE

COMPLIANCE 231	COMPLIANCE 679
1) Principio di responsabilità oggettiva dell'Ente;	1) Principio di <i>accountability</i> del Titolare del trattamento;
2) Mappare i processi operativi;	2) Mappare i trattamenti di dati personali;
3) Valutare il rischio di reati che potrebbero essere commessi nei vari processi aziendali;	3) Valutare i rischi derivanti dal trattamento dei dati personali per gli interessati;
4) Stabilire procedure per evitare che tali reati vengano commessi;	4) Stabilire procedure per evitare o rimediare ad eventuali violazioni (ad es. data breach policy);
5) Necessità di definire ruoli e responsabilità (principio di separazione dei poteri);	5) Necessità di stabilire i ruoli e le responsabilità (autorizzato, responsabile, contitolare);
6) Obbligo di creare un organo di controllo (Organismo di vigilanza);	6) Obbligo (sopra certi parametri) di nominare un organo di controllo (Responsabile Protezione Dati);
7) Formazione obbligatoria a tutti coloro ai quali si applica il MOG.	7) Formazione obbligatoria per tutti gli autorizzati.

ANALOGIE E MISURE ATTUATIVE: REATI INFORMATICI E DATA BREACH

ART. 24 bis - 231/2001	ART. 32 – 2016/679
<p>1. «Delitti informatici e trattamento illecito di dati» (artt. 615 ter, 615 quater e 615 quinquies, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater e 635 quinquies, 491 bis e 640 quinquies del Codice penale) sono tutti interpretabili come violazioni ex art. Art. 4 par. 1 n. 12 del GDPR ;</p> <p>2. Misure e protocolli per prevedere e prevenire tali reati.</p>	<p>1. Tenendo conto [...] del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e [...] mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;</p> <p>2. Stabilire procedure per evitare o rimediare ad eventuali violazioni (ad es. data breach policy).</p>

Quali, ad esempio: nomine ad autorizzato e relative istruzioni operative (ad es. *segregazione degli accessi*), politica sulle violazioni (*con albero decisionale*), individuazione figure di riferimento per la singola Business Unit (*referenti privacy interni*) in caso dubbi, da parte degli autorizzati, sulle *best practices* della società e su potenziali violazioni, regolamento per i *device (inclusi eventuali dispositivi per la doppia autenticazione)*, valutazioni d'impatto ex art. 35.

GRAZIE PER LA VOSTRA ATTENZIONE

Avv. Matteo Alessandro Pagani: pagani@plslegal.eu

Dott. Alessandro Burro: alessandro.studio.burro@gmail.com

PLS LEGAL: legal@plslegal.eu

PLS: privacy@gruppopls.com

Sito Web: www.gruppopls.com

