ANDERSEN®

luglio 2026

&Compliance Risk Management

Novità normative e pratiche di governance dei dati e di gestione di rischi d'impresa

Paola Finetto
Partner
paola.finetto@it.andersen.com

Luca Rigotti
Partner
luca.rigotti@it.andersen.com

Hanno collaborato: **Nicolò Bottura**, **Elisa D'Arrigo** e **Edoardo Vittorio Lazzaro**

D.Lgs. 231/2001

Quando il controllo delle e-mail del dipendente può diventare un reato presupposto ai sensi del D.Lgs. 231/2001

L'accesso alle e-mail aziendali dei dipendenti non è sempre lecito. In determinate circostanze, le modalità con cui l'azienda monitora la posta elettronica di un dipendente possono integrare reati rilevanti ai fini della **responsabilità dell'ente** ex D.Lgs. 231/2001.

Il rischio si manifesta quando un dirigente, senza titolo, **accede alla mail** di un dipendente, **utilizza credenziali** conosciute o recuperate senza consenso, **mantiene l'accesso** alla casella dopo la cessazione del rapporto di lavoro, **monitora** sistematicamente le mail o **acquisisce** il contenuto delle e-mail in assenza dei presupposti previsti dalla legge.

Tali condotte possono integrare i reati di accesso abusivo a un sistema informatico o di intercettazione illecita di comunicazioni informatiche, entrambi inclusi tra i reati che possono determinare la **responsabilità dell'ente ex art. 24-bis D.Lgs. 231/2001**.

Il rischio per l'ente aumenta quando i controlli vengono effettuati per **acquisire informazioni** riservate sul dipendente, **prevenire contestazioni**, raccogliere elementi da utilizzare in procedimenti disciplinari o **ottenere vantaggi organizzativi** per la società.

Procedure di controllo poco chiare, assenza di autorizzazioni formalizzate e carenze nei protocolli informatici possono trasformare un'attività di verifica interna in un significativo rischio 231: la prevenzione passa da **policy chiare, autorizzazioni documentate e formazione mirata**.

Privacy | AI | Cyber

E-mail aziendale: la necessità di una procedura per un utilizzo GDPR compliant

Molte imprese considerano ancora le e-mail di lavoro come un semplice strumento operativo, dimenticando che i messaggi contengono in realtà grandi quantità di dati personali (anche sensibili) relativi a dipendenti, clienti e fornitori. Senza una precisa regolamentazione interna, il **rischio di non essere conformi alla normativa privacy** è molto alto per qualsiasi realtà imprenditoriale, indipendentemente dalle dimensioni.

Il Garante per la protezione dei dati personali ha più volte ribadito che il datore di lavoro non può mai controllare indiscriminatamente la corrispondenza dei dipendenti.
Anche dopo la cessazione del rapporto lavorativo, l'account non può rimanere attivo a tempo indeterminato e la posta non può essere reindirizzata automaticamente a un superiore in modo sistematico.

Tali prassi, infatti, non rispettano i **principi di minimizzazione, trasparenza e limitazione della conservazione** dei dati previsti dal Regolamento Europeo.
Per prevenire incidenti di sicurezza, nonché per evitare contenziosi o sanzioni, ogni organizzazione deve adottare una specifica **procedura per l'utilizzo della posta elettronica**.

Tale policy aziendale deve definire le corrette **modalità d'uso della casella di posta elettronica, le caratteristiche delle credenziali di accesso all'account di posta elettronica, i tempi massimi di conservazione** della corrispondenza, le **modalità di accesso** da parte dell'azienda, i casi in cui possono essere effettuati **controlli** in conformità alla normativa privacy e alla normativa in materia di diritto del lavoro, **la gestione degli account cessati** e le **conseguenze di condotte non conformi**.

Una gestione consapevole e conforme dell'e-mail aziendale rappresenta una tutela fondamentale per il patrimonio informativo e la reputazione del business. Implementare una procedura interna riduce i rischi legali e trasforma la compliance in un concreto vantaggio sul mercato.

Risk Management

Individuare e mitigare i rischi di attacco informatico veicolato tramite e-mail

L'e-mail continua a rappresentare uno dei principali vettori di attacco informatico.

Campagne di phishing e diffusione di malware sfruttano sempre più il **fattore umano**, inducendo gli utenti a divulgare informazioni riservate, compromettere credenziali o autorizzare operazioni fraudolente, anche soltanto con un "clic" sull'allegato o sul link trasmessi a mezzo e-mail.

La gestione di questo rischio non può essere affidata esclusivamente agli strumenti tecnologici.

Essa richiede un sistema di **governance** che integri misure tecniche, organizzative e procedurali, fondato su una preventiva **valutazione dei rischi** e su una chiara attribuzione di ruoli e responsabilità.

La **formazione** continua del personale, l'adozione di procedure di verifica per le richieste anomale, la definizione di **protocolli di risposta** agli incidenti e il periodico riesame delle misure adottate costituiscono elementi essenziali di un modello di **sicurezza** efficace e resiliente.

In un contesto normativo che attribuisce crescente rilievo alla **resilienza informatica** e all'**accountability** delle organizzazioni (tra cui, AI Act, DORA, NIS2, CER, GDPR), la sicurezza delle comunicazioni elettroniche non rappresenta soltanto un presidio tecnico, ma un fattore di corretta governance e di tutela del patrimonio informativo aziendale.