La Relazione annuale del DPO: l'importanza per il Titolare

Security Governance & Data Protection

29 marzo 2023

sogei

Principali punti di attenzione

1. Compliance normativa
2. Regole di *soft law*
3. La *legal compliance* in Sogei
4. Compliance privacy – il ruolo del DPO
5. Attività di Reporting del DPO
6. La Relazione Annuale al CdA
7. L'esperienza di Sogei – gli standard di rendicontazione
8. L'esperienza di Sogei – la relazione annuale al CdA

Relazione annuale del DPO (1/5)

1. Compliance normativa

La conformità normativa o *legal compliance* è un unitario sistema di gestione e deve essere considerata in un unico contesto di procedure interconnesse e coordinate.

ELEMENTI DI LEGAL COMPLIANCE:

- assunzione di regole interne richieste dalla legge al fine di raggiungere la conformità dei processi e dei sistemi aziendali;
- assetto dei sistemi di governance che persegua la tutela dei beni strategici;
- tendenza allo zero di situazioni patologiche.

2. Regole di *soft law*

La *soft law* in generale detta le norme tecniche e/o di dettaglio con cui garantire la protezione di alcuni diritti, interessi o beni giuridici fondamentali.

LE AUTORITA' CHE DETTANO LE REGOLE DI SOFT LAW:

- Ruolo primario è riservato alle Authority e, in particolare, al Garante per la protezione dei dati personali;
- Altri soggetti che governano l'informatica e l'innovazione in ambito pubblico:
  - Presidenza del Consiglio – Dipartimento per la trasformazione digitale;
  - Agenzia per l'Italia Digitale (AgID)
  - Autorità per la Cybersicurezza Nazionale (ACN)
  - Altre Amministrazioni centrali

3. La *legal compliance* in Sogei

In Sogei è attivo un complesso sistema di controllo interno attuato attraverso una pluralità di organi e con specifiche strutture organizzative dedicate, che si compone di codici comportamentali, sistemi di gestione, policy e procedure, che costituiscono un dominio, oggetto di costante monitoraggio e adeguamento all'evoluzione del contesto normativo, istituzionale e operativo nel quale opera la Società.

Si tratta di un sistema di controllo dei rischi che è in costante aggiornamento e miglioramento.

Relazione annuale del DPO(2/5)

4. Compliance Privacy – il ruolo del DPO

Il DPO, che è parte integrante di un più complesso sistema di compliance, deve garantire la conformità dei processi aziendali - e dei trattamenti a questi connessi – alle disposizioni in materia di protezione dei dati personali, supportando il titolare, o il responsabile, nell'attuazione pratica di un sistema di regole, procedure e controlli con particolare attenzione al profilo della sicurezza dei trattamenti di cui all'art. 32 del GDPR.

DOVERE DI INFORMAZIONE E CONSULENZA AL TITOLARE Art. 39 GDPR

Per garantire la compliance e supportare il titolare nel raggiungimento di uno scenario ottimale di conformità il DPO deve:

- rendicontare il proprio operato e informare sullo stato di adeguamento;
- suggerire l'implementazione di eventuali azioni di miglioramento;
- formulare un parere non vincolante sulla DPIA (Valutazione di impatto privacy – art. 35 GDPR);
- formulare un parere in merito alla struttura, all'impostazione e all'amministrazione della documentazione relativa al data breach (art. 33 GDPR).

5. Attività di reporting del DPO

Nell'ambito dei compiti di informazione e consulenza previsti dall'art. 39, il DPO svolge una fondamentale attività di reporting, che si traduce in un prezioso strumento di accountability.

RIFERIMENTI NORMATIVI DELL'ATTIVITÀ DI REPORTING DEL DPO

- Art. 2381 comma 5 c.c.;
- Vecchio Allegato B al Codice Privacy (Dlg 196/2003);
- Art. 38 comma 3 GDPR «*Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*»;
- Linee Guida del WP29 sui Responsabili della Protezione dei Dati (WP243);
- Art. 27 dello Statuto sociale di Sogei;
- Manuale RPD - Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e para-pubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea
- FAQ Garante Privacy

Relazione annuale del DPO(3/5)

6. La Relazione Annuale al CdA

«Un monitoraggio attento e regolare della conformità e la presentazione dei risultati possono esercitare una forte pressione sui titolari per garantire la conformità delle loro operazioni di trattamento. Il ***monitoraggio periodico*** *e il* ***reporting dei risultati*** *sono l'arma più forte a disposizione del RPD per garantire la conformità e, a questo scopo,* ***una relazione annua*** *destinata alle alte dirigenze costituisce un'ottima prassi».*

(Manuale RPD)

L'obiettivo della relazione annuale è quello di fornire al Consiglio di Amministrazione una panoramica delle attività svolte dal DPO in merito ai compiti assegnati e con riferimento agli interventi effettuati in esecuzione delle attività programmate per l'anno di riferimento.

LA RELAZIONE CONSENTE AL TITOLARE DI:

- valutare lo stato di maturità del percorso aziendale;
- verificare l'adeguatezza delle scelte effettuate;
- indirizzare gli investimenti aziendali necessari, anche in considerazione delle mutazioni in corso del contesto normativo, di business e tecnologico.

LA RELAZIONE CONSENTE AL DPO DI:

- documentare l'implementazione delle azioni pianificate;
- illustrare eventuali interventi ulteriori necessari al fine di migliorare l'organizzazione aziendale, che quindi saranno inseriti nel piano di attività per l'anno successivo;
- dimostrare l'attenzione al costante aggiornamento normativo e alle pronunce del Garante Italiano ed europeo.

Relazione annuale del DPO(4/5)

7. L'esperienza in Sogei – gli standard di rendicontazione

L'attività di reporting del DPO, interconnessa con le diverse normative di compliance che presentano elementi di interferenza con la protezione dei dati personali, si inserisce nei più generali obblighi di compliance che regolano le norme di impresa, tradotte nell'ESG (Environmental, Social, and corporate Governance). Di recente è stato esteso l'ambito di applicazione dell'obbligo di reporting non finanziario sulla sostenibilità dalla Direttiva 2022/2464 – CSRD (Corporate Sustainability Reporting Directive) del 14 dicembre 2022.

Il DPO ha il dovere di offrire la propria consulenza, di formulare pareri e informare alcuni dei principali organi aziendali interessati dalla compliance, quali: (i) il Responsabile della Prevenzione Corruzione e Trasparenza (RPCT), (ii) gli organi di controllo (OdV, Collegio Sindacale, OIV, Internal Auditing), (iii) la Direzione "Affari Legali e Procurement", (iv) il Direttore "Security, Safety & Industrial Relations".

L'attività di reporting del DPO di Sogei si estende, nell'ambito della corporate governance, al bilancio integrato - nel quale confluiscono il bilancio di esercizio e il bilancio di responsabilità sociale d'impresa - che si compone di alcune sezioni espressamente dedicate al sistema di governo della sicurezza delle informazioni, data protection e all'etica digitale.

STANDARD UTILIZZATI PER LA RENDICONTAZIONE

L'attività di reporting di Sogei - tanto la relazione annuale del DPO al CdA quanto il bilancio integrato - risponde agli Standard GRI per la rendicontazione della sostenibilità e, per quel che qui interessa, al "GRI 418: Customer Privacy 2016", in abbinamento alle informazioni richieste dalla "Disclosure 3-3: Gestione degli argomenti rilevanti", i quali richiedono di inserire le seguenti informazioni circa:

- Le azioni, le politiche, gli impegni assunti dalla società per migliorare la protezione dei dati personali;
- I processi interni per monitorare il raggiungimento degli impegni e degli obiettivi in materia di protezione dei dati personali;
- Le procedure operative presenti in materia di protezione dei dati personali;
- il numero totale di reclami ricevuti in merito a violazioni della privacy degli interessati;
- il numero totale di fughe, furti o perdite di dati (data breach) degli interessati.

Relazione annuale del DPO(5/5)

8. L'esperienza in Sogei – La Relazione Annuale al CdA

La Relazione del DPO di Sogei si compone di sei sezioni nelle quali sono indicate le principali attività svolte dal DPO e si conclude con il rilevamento dello stato di maturità aziendale. Vale la pena ricordare i principali interventi posti in essere da Sogei nel 2022.

PRINCIPALI INTERVENTI 2022

- Sogei ha prestato particolare attenzione al settore della sicurezza e, nell'ambito di un programma di monitoraggio delle conformità ex art. 32, ha sottoposto ad analisi privacy by design i servizi ICT che trattano dati personali, interni ed erogati alle amministrazioni clienti.
- per attuare la propria strategia cloud volta a realizzare un Hybrid Multicloud Data Center, da offrire ai soggetti pubblici, Sogei ha dato avvio all'attività di negoziazione con alcuni dei maggiori Cloud Service Provider (CSP) per l'acquisizione di tale tipologia di soluzioni tecnologiche. Tale attività ha richiesto particolari punti di attenzione soprattutto con riferimento al trasferimento dei dati extra UE.
- la struttura Data Protection Governance ha provveduto alla redazione di nuova documentazione privacy e all'aggiornamento di quella già esistente, al fine di
  - adeguare il Sistema di gestione della Privacy alle novità normative e di contesto;
  - ampliare la copertura rispetto alle prescrizioni del GDPR;
  - rafforzare l'efficacia dell'intero sistema di gestione della privacy.

STATO DI MATURITA' 2022

- miglioramento generale in termini di conformità al GDPR rispetto all'anno precedente
- maturità aziendale dei processi GDPR notevolmente superiore al 2021