

# Verifiche Ispettive Garante

A cura di

**Supporto Normativo Protezione dei Dati Personali**

Milano, 16 febbraio 2023



# La Verifica ispettiva

L'Autorità Garante per la protezione dei dati personali si occupa di **constatare**, tramite delle verifiche ispettive, **lo stato di conformità alla Normativa Privacy (come previsto dall'Art. 80 GDPR)**. Le verifiche ispettive riguardano gli aspetti fondamentali sanciti dal GDPR nella gestione della privacy.

L'Ispezione del Garante **rappresenta un momento di grande stress e importante tensione** all'interno dell'organizzazione sottoposta alle verifiche.



L'Ispezione del Garante rappresenta **un momento formativo, di crescita per l'organizzazione.**

Dopo la chiusura dell'attività di Verifica Ispettiva, è fondamentale per l'organizzazione **discutere e confrontarsi** per **individuare le «Lessons Learned»**, al fine di  **cogliere spunti di miglioramento** da adottare nel sistema privacy aziendale.

# Gestione della Verifica Ispettiva - Fasi

Sulla base delle esperienze precedenti, ARIA ha individuato tre momenti fondamentali che vengono gestiti durante la Verifica Ispettiva. In particolare:



**Accoglienza:** fase preliminare di introduzione del procedimento



**Verifica dei trattamenti:** analisi del Registro, della documentazione a corredo, degli adempimenti richiesti, delle misure di sicurezza. Verifiche sostanziali e non formali








**Conclusioni:** Condivisione e verbalizzazione dei risultati

# Gestione della Verifica Ispettiva – Accoglienza e Presentazione

Le visite dell'Autorità Garante possono avvenire tramite preavviso, come previsto dal Codice Privacy, o a sorpresa. In particolare **nel secondo caso l'autorità** può presentarsi **direttamente al desk** o alla **reception di ingresso**.

Attraverso esperienze pregresse, **è consigliato, nelle fasi iniziali, svolgere le seguenti azioni:**

-  **Gestire** correttamente le **procedure di accoglienza** e la **condivisione della checklist di contatto**;
-  Coinvolgere le **figure apicali** e **predisporre eventuali deleghe**;
-  Costituire il **team a supporto della verifica ispettive**;
-  Coinvolgere il **DPO**;
-  Predisporre l'**eventuale informativa al titolare**.

# Gestione della Verifica Ispettiva - Registro dei Trattamenti

Solitamente le ispezioni del Garante **possono focalizzarsi su uno o più trattamenti**.

Durante la Verifica Ispettiva risultano importanti **i seguenti aspetti**:



- **Corretta manutenzione del Registro dei Trattamenti**

- Sviluppare **flussi di dati collegati** ad altri strumenti a disposizione dell'organizzazione;
  - **Dotarsi di un Data Catalog e/o mappe delle relazioni** tra i diversi database;
  - Predisporre descrizioni dei processi, soprattutto in termini di **Segregation of duties**;
  - **Gestire** correttamente e in maniera preventiva le **possibili minacce legate al trattamento**;
  - **Verificare e gestire** correttamente l'applicazione delle **Misure di Sicurezza sui relativi sistemi**.
- 
- Coinvolgere l'**Owner del trattamento**;
  - Raccogliere la **documentazione fondamentale per rispettare il principio di Accountability** che permette di consolidare e dimostrare un **sistema privacy efficace**;
  - Gestione delle **terze parti coinvolte**.

# Gestione della Verifica Ispettiva - Esempi di richieste

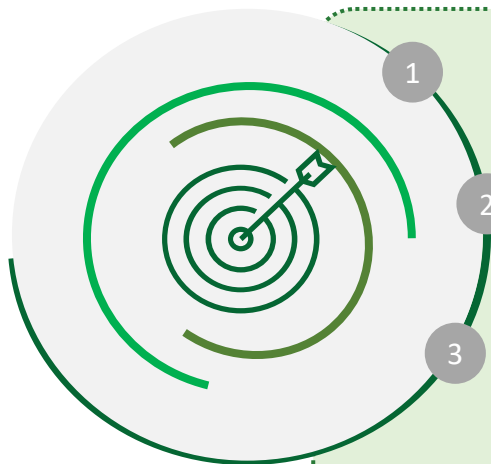
Essere in **grado di eseguire una serie di operazioni è fondamentale** per rispondere **in modo preciso e tempestivo** ad una serie di possibili richieste, tra cui:

- 1 Quanti dati sono contenuti nel sistema?
- 2 A quanti interessati appartengono?
- 3 Quale è il dato più vecchio presente sul sistema?
- 4 Quale è il numero di utenti abilitati sul sistema?
- 5 Quale è il numero di gruppi abilitati sul sistema?
- 6 Quale è il numero di utenti per ciascun gruppo?
- 7 Quali sono i flussi logici tra le diverse applicazioni?
- 8 Quali e quante banche dati contengono un determinato dato?
- 9 In che modo vengono aggiornati?

L'Organizzazione, **attraverso controlli periodici**, sui processi automatizzati e ottimizzati **è in grado di recuperare le evidenze** richieste dal Garante.

# Gestione della Verifica Ispettiva - Conclusione

La conclusione della **Verifica ispettiva** è un momento importante per:



1 **Avere chiaro il punto della situazione** e delle criticità emerse

2 Mettere in atto **azioni correttive** adeguate

3 **Integrare eventuale documentazione**, richiesta dal Garante, a valle della Verifica Ispettiva

# Preparazione alle Ispezioni (1/2)

Per affrontare con **professionalità e competenza** un **Ispezione del Garante** è fondamentale **l'attività di formazione e sensibilizzazione del personale**.



## AWARENESS & FORMAZIONE

L'attività prevede sessioni formative e redazione di contenuti di tipo documentale inerenti alle tematiche privacy che vengono condivise con le figure aziendali preposte alla gestione della stessa.



## SIMULAZIONI

L'attività prevede sessioni di simulazione dell'attività di «Ispezione» al fine di verificare la prontezza dell'organizzazione di fronte ad eventuali ispezioni programmate e non.



# Preparazione alle ispezioni (2/2)

Per gestire al meglio le situazioni di «Stress», conseguenti l'attività di verifica e minimizzare il rischio di errori, risulta di fondamentale importanza essere preparati alle Visite Ispettive.

A tal proposito, **ARIA** ha pianificato una **metodologia di Privacy Stress Test** che prevede la simulazione di uno scenario reale di ispezione per verificare se il proprio gruppo di lavoro fosse in grado di rispondere, in modo coerente e tempestivo, alle richieste avanzate dal gruppo ispettivo.

## Come vengono gestite le attività di simulazione della Verifica Ispettiva?



**Modalità:** gestita, ad esempio, table -top



**Soggetti Coinvolti:** durante la simulazione i soggetti possono ricoprire il Ruolo di «Ispettore» e Titolare/Responsabile del Trattamento. Altresì, possono essere coinvolte anche le Terze Parti;



**Verifiche:** le verifiche si basano sulle tre fasi fondamentali del procedimento (**Accoglienza – Verifica dei Trattamenti e adempimenti – Fase conclusiva**);



**Debriefing:** condivisione dei risultati e discussione dei punti di miglioramento derivati dalla simulazione.

# Risultati raggiunti

