A Angelo Colombi

I A tutti gli interessati

Ispezione G.d.F. in materia di privacy

L'ispezione in materia di privacy è un'attività volta a verificare che i dati personali di cui l'organizzazione è in possesso, siano trattati secondo quanto previsto dal Regolamento Europeo 2016/679 (GDPR).

Quello che viene richiesto al titolare in sede ispettiva è comprovare l'accountability, ovvero l'attuazione di misure tecniche e organizzative opportune, efficaci e adeguate per la salvaguardia dei dati personali trattati. **Questo significa**, fondamentalmente, **non solo divenire responsabili delle procedure e dei mezzi** scelti in materia di trattamento dei dati, **ma anche di essere in grado di "dare conto" delle valutazioni** che stanno alla base delle scelte poi operate.

L'importanza dell'accountability emerge soprattutto in fase di controllo del Garante dove **l'azienda o il professionista dovrà dimostrare agli ispettori, con ragionamento logico e documentato, quanto ha fatto concretamente per adempiere alla normativa** ed eventualmente difendersi da **scelte opinabili quali ad esempio il non aver nominato un Data Protection Officer** o **non aver predisposto il registro dei trattamenti**. Al termine dell'ispezione l'organizzazione potrà valutare se si sta agendo in modo adeguato al regolamento europeo o se si stanno trascurando azioni importanti.

Gli accertamenti ispettivi possono scaturire a seguito di segnalazioni o reclami dei soggetti interessati oppure d'ufficio su iniziativa del Garante, ad esempio in base alla pianificazione semestrale dei controlli.

Le attività ispettive sono condotte dal Nucleo Speciale Privacy della Guardia di Finanza e nei casi più gravi da funzionari del Garante i quali procedono personalmente alle ispezioni con o senza il supporto della GdF.

L'attività ispettiva su iniziativa del Garante è a cura del personale dell'Ufficio o delegato alla Guardia di finanza e ricomprende l'accertamento nei luoghi dove si effettuano i trattamenti di

dati, o, in alternativa, può avvenire tramite convocazione presso l'Autorità e in questo caso è disposta da un ordine di servizio.

Le ispezioni possono essere "**annunciate"** dal Garante o dalla GdF tramite una comunicazione, spesso solo il giorno prima dell'arrivo, così come **possono avvenire a sorpresa**. Nel primo caso la comunicazione viene fatta a mezzo PEC ed è opportuno che chi legge avverta subito i vertici aziendali, quindi la funzione legal e/o compliance in modo da prepararsi all'arrivo degli ispettori.

Quale che sia il soggetto ispettore, il perimetro dell'ispezione è individuato da un documento che viene notificato al momento dell'accesso in sede: si tratta della "richiesta di informazioni" con cui il Garante domanda come siano stati assolti determinati obblighi legislativi o regolamentari in materia di protezione dei dati personali.

La richiesta di informazioni può includere: modalità con cui viene data l'informativa agli interessati, modalità di raccolta del consenso – ove necessario –, come vengano contrattualizzati i responsabili esterni del trattamento, quali siano le misure di sicurezza tecniche e organizzative adottate, data retention policy dei dati trattati, la formazione erogata agli autorizzati del trattamento dei dati eccetera.

Indice degli argomenti

L'utilizzo di un documento contenente una procedura di gestione dell'ispezione, con ruoli e comportamenti da seguire in fase di controllo, è sempre utile per non farsi prendere dal panico in momenti come questi in cui l'emotività può giocare brutti scherzi anche alle aziende più compliant.

In generale, comunque, il consiglio è sempre quello di mostrarsi collaborativi con gli ispettori; atteggiamenti ostili sono decisamente controproducenti.

L'obbligo di collaborazione implica il dovere di fornire l'accesso a documenti cartacei ed elettronici contenuti in computer, hard disk e in ogni altro dispositivo informatico, l'obbligo di

indicare dove sono conservati i documenti d'interesse nonché l'obbligo di fornire ogni informazione richiesta indipendentemente dal fatto che i documenti o le informazioni siano tenute in luoghi diversi o da soggetti diversi dal titolare quali responsabili del trattamento.

1. Come si svolge l'attività ispettiva

Le ispezioni durano mediamente 1-3 giorni, è consigliabile che almeno una delle persone individuate per la gestione dell'ispezione sia presente per tutto il tempo in modo da coordinare i lavori e fare da punto di riferimento sia interno che per gli ispettori.

Al termine dell'attività ispettiva è importante verbalizzare quanto emerso e, se ritenuto opportuno, mettere a verbale dichiarazioni di cui si desidera lasciare traccia. **In caso di dubbio, non rispondere è meglio che dare informazioni false**. È fondamentale, inoltre, riservarsi sempre di esaminare la correttezza di quanto dichiarato e far vagliare le dichiarazioni messe a verbale da un consulente privacy esterno in modo da verificare che non si rivelino controproducenti o contraddittorie.

2. Ispezione privacy: suggerimenti pratici

Alla luce di quanto detto è quindi opportuno mettere in pratica alcuni suggerimenti pratici in modo da affrontare al meglio una eventuale ispezione privacy:

- farsi rilasciare sempre copia del verbale d'ispezione;
- prendere nota di tutti i documenti (incluse banche dati, archivi, sistemi informatici) visionati dagli ispettori;
- segnare tutte le informazioni richieste e fornite;
- rilasciare solo copie e mai documentazione in originale.

Va da sé che maggiore sarà la compliance privacy dell'organizzazione maggiore sarà la facilità nel soddisfare le richieste dell'Autorità.

3. Ispezione privacy: documenti e informazioni più richieste

Tipicamente, durante un'ispezione privacy verranno richiesti i seguenti documenti privacy:

- registro dei trattamenti;
- nomina del Data Protection Officer (DPO);

- nomine dei responsabili del trattamento;
- la formazione per gli autorizzati al trattamento dei dati;
- informative;
- data retention policy;
- DPIA (Data protection impact assessment);
- registro dei data breach.

Il primo documento oggetto di analisi da parte dell'Autorità di controllo è il registro dei trattamenti; questo documento deve contenere l'inventario di tutti i trattamenti di dati personali eseguiti dall'azienda. È considerato indice di una corretta gestione dei trattamenti, per tale motivo dovrà essere sempre aggiornato, chiaro, completo e aderente alla realtà attuale dell'azienda. L'aggiornamento deve recare "in maniera verificabile" sia la data della sua prima istituzione sia la data del suo ultimo aggiornamento.

È necessario, inoltre, che quanto riportato su tale documento sia in linea con quanto indicato nelle diverse informative sulla privacy adottate dall'organizzazione.

Spesso, purtroppo, le informative vengono considerate come dei formulari standard contenenti informazioni parziali, se non del tutto errate. Questo può esporre l'azienda al rischio di contestazioni da parte del Garante. **La mancata corrispondenza tra i trattamenti di dati personali svolti dall'azienda e quelli indicati nella documentazione privacy può essere facilmente verificata dagli ispettori, così come la non veridicità delle informazioni riportate all'interno della documentazione stessa.**

La problematica non va sottovalutata, in quanto può comportare **responsabilità penali**. La falsità nelle dichiarazioni rese all'Autorità viene infatti sanzionata dal Codice Privacy con la **reclusione da 6 mesi a 3 anni**. Quindi, in sede di ispezione, esibire documenti che non rappresentano le effettive attività di trattamento svolte dall'azienda (in particolar modo per il Registro dei trattamenti), aumenta il rischio della contestazione di tale reato.

Dal registro, se bene compilato, sarà possibile disegnare una mappa immediata dei flussi di dati in entrata e in uscita, dei relativi responsabili oltreché delle misure di sicurezza adottate. In base poi al processo dichiarato, se ne valuterà la gestione, anche dal lato informatico.

Anche avere un Modello Organizzativo Privacy può aiutare a dimostrare l'accountability del titolare. Dotarsi di un modello organizzativo valido, infatti, significherebbe non solo aiutare

l'azienda a garantire il rispetto della normativa, ma anche avere un maggior controllo delle proprie attività ed economie di scala.

Registro alla mano si procederà poi ad effettuare gli ulteriori controlli fra cui, se prevista, la nomina del Data Protection Officer (DPO) per poi passare alla nomine dei responsabili (ex art. 28 GDPR) e in particolare, alla verifica delle relative istruzioni sul trattamento impartite dal titolare mediante contratti o atti giuridici.

Per quanto riguarda il **DPO è opportuno che sia presente durante le ispezioni**, il Garante non apprezza la nomina di un DPO che non sia facilmente raggiungibile. La mancata partecipazione del DPO in sede ispettiva o il fatto che questi non sia sufficientemente informato sulle attività effettuate dall'organizzazione potrebbe portare l'Autorità a ritenere che l'azienda non sia in grado di esercitare un controllo effettivo sui trattamenti dei dati personali eseguiti.

È facile dedurne che il Garante e i funzionari della GdF, adottando un approccio sostanziale in sede ispettiva, **non si accontenteranno della mera esibizione di documenti privi di sostanza** ma verificheranno quali effettivamente siano le attività di trattamento dei dati personali svolte e le regole adottate.

In sede ispettiva, infatti, il Garante, in diversi casi, ha richiesto di acquisire **il programma ed il piano di formazione**, i materiali erogati, il test finale ed ha analizzato il profilo delle istruzioni agli incaricati al trattamento connesse all'accesso, alla consultazione delle banche dati, i livelli di autorizzazione e le policy aziendali (ad esempio in materia di password aziendali e di videosorveglianza); il tutto verificando la reale preparazione del personale addetto.

La formazione è un elemento fondamentale per le organizzazioni, in quanto costituisce una misura di sicurezza oltreché un diritto e dovere per dipendenti e collaboratori.

Altro elemento imprescindibile è avere le informative in regola, solo così potrà essere garantito all'interessato il principio di trasparenza**. L'informativa dovrà quindi essere chiara**, sintetica, avere i contenuti previsti dalla legge, essere facilmente consultabile (sul sito web e da remoto), e deve essere comprensiva di tutti i trattamenti effettuati dall'azienda. Ove necessario, anche la raccolta del consenso al trattamento dei dati, dovrà essere ben gestito; dovrà quindi essere provata la modalità di raccolta e la conservazione dello stesso. Questo anche in un'ottica di richiesta di esercizio dei diritti da parte dell'interessato.

Per quanto riguarda la **gestione dei tempi di conservazione dei dati**, è opportuno fare una precisazione. Anzitutto è essenziale definire il tempo di conservazione di un dato legandolo alla finalità del trattamento nel quale è coinvolto, di conseguenza, se lo stesso dato è trattato per diverse finalità, si dovranno stabilire tempi di conservazione differenti in funzione di ognuna delle diverse finalità.

Tuttavia, quello che spesso viene tralasciato sono i diversi supporti sui quali i dati personali sono di norma conservati (digitale, analogico ecc.) i quali, non sempre si trovano presso la struttura del Titolare, pensiamo agli outsourcer e ai fornitori.

Gli ispettori richiederanno la valutazione d'impatto (DPIA) o il fondamento delle ragioni che ne hanno escluso l'adozione; **occorre quindi individuare con cura tutti quei trattamenti che, in base alle indicazioni del GDPR, necessitino di una valutazione d'impatto**, soprattutto nei casi palesi di sorveglianza e videosorveglianza su larga scala, profilazione, geo-localizzazione e trattamento di dati particolarmente delicati.

In caso di esternalizzazione dei dati, poi, **potrà essere richiesta la collaborazione del responsabile esterno** per avere in mano tutte le informazioni necessarie per redigere la valutazione stessa.

Uno dei motivi principali da cui potrebbe derivare un'ispezione privacy è la mancata notifica al Garante di una violazione dei dati personali (c.d. data breach) di cui l'Autorità sia venuta comunque a conoscenza, ad esempio tramite un reclamo presentato all'Autorità stessa, o l'avvenuta notifica di un data breach su cui il Garante intenda ottenere maggiori informazioni.

È opportuno, quindi, assicurarsi che ci sia una dettagliata procedura interna su come gestire una violazione di dati (ivi incluso l'iter comunicativo e le azioni da porre in essere) e che tale procedura preveda anche gli obblighi cui sono tenuti i fornitori di servizi eventualmente coinvolti dal data breach e la relativa formazione al personale.

Sicuramente, adottare politiche di protezione testate, che consistono non solo nel decidere in 72 ore "se notificare", ma anche quali sono le misure di mitigazione da porre in essere, per l'azienda e per l'interessato, al fine di ridurre rischi e conseguenze del breach, è dimostrazione di accountability.

Fra i consigli pratici da implementare abbiamo: l'adozione di un protocollo di risposta, testare periodicamente il protocollo per controllarne la validità; dotarsi di una copertura assicurativa per

eventuali data breach; tenere un registro dei casi di data breach; compiere un'attività di indagine volta ad individuare la natura e la portata della violazione.

4. Regole fondamentali per affrontare al meglio l'ispezione privacy

Fra le regole necessarie per gestire correttamente un'ispezione privacy vi è senz'altro – come abbiamo già visto – quella di avere una procedura interna chiara per affrontare le ispezioni, prevedendo le azioni da intraprendere durante le diverse fasi dell'indagine e, in particolare:

- individuare i principali interlocutori dell'Autorità (non solo il DPO, ma anche il consulente esterno per la privacy e il contatto in ogni ufficio dell'azienda) con istruzioni specifiche;
- definire quale procedura deve essere adottata e quali documenti relativi alla protezione dei dati devono essere consegnati all'Autorità;
- formare il personale indicando come gestire le richieste formulate dall'Autorità.

1. Governance della protezione dei dati

Responsabilità della protezione dei dati, politiche, procedure, controlli di misurazione della performance e meccanismi di controllo per monitorare la conformità: sono in funzione? In che misura? E' stato fatto l'organigramma della Privacy aziendale?

2. Gestione dei rischi

Il rischio di privacy è incluso nel registro dei rischi aziendali? Quali accordi aziendali sono in atto per la gestione del rischio della privacy all'interno della tua impresa? In che misura il regime di rischio societario incorpora rischi specifici delle informazioni? Quali sono i rischi presi in considerazione per i diritti e le libertà delle singole persone?

3. Progetto GDPR

Il progetto di adeguamento GDPR in atto è adeguatamente supportato ed in grado di raggiungere obiettivi realistici?

4. Responsabile della protezione dei dati (DPO)

Nel caso in cui un DPO sia obbligatorio, è stato nominato ed il ruolo integrato nell'organigramma? La persona nominata è in grado di soddisfare i requisiti del GDPR?

5. Ruoli e responsabilità

Come sono definiti i ruoli e le responsabilità in tutta l'organizzazione? Sono stati predisposti i documenti di nomina, consegnati e firmati? Come viene affrontata la questione della formazione del personale?

7. Ambito di applicazione

È essenziale che l'ambito di applicazione sia definito in modo chiaro, identificando e aggiornando il registro dei trattamenti (ad esempio è stato creato il nuovo trattamento dei dati in riferimento al trattamento del green pass?

8. Analisi del processo

Per ogni processo che coinvolge i dati personali è importante identificare come sono stabiliti i principi di elaborazione dei dati, ossia la base legale al trattamento. Ci sono processi per i quali una valutazione d'impatto della protezione dei dati (DPIA) è obbligatoria, e per quali processi una DPIA potrebbe contribuire a stabilire la protezione dei dati fin dalla progettazione e per impostazione predefinita?

8. Sistema di gestione delle informazioni personali

Esiste un'ampia gamma di documentazione necessaria per garantire che la tua impresa sia in grado di dimostrare la conformità al GDPR, per esempio una politica di protezione dei dati, una procedura di notifica di violazione, moduli e procedure per la richiesta di accesso, DPIA, moduli per le informative e il consenso. La quantità di documentazione deve essere adeguata alle dimensioni ed alla complessità dell'organizzazione. Il sistema di gestione delle informazioni personali dovrebbe anche considerare la formazione e la sensibilizzazione del personale.

9. Sistema di gestione della sicurezza delle informazioni

Verifica le misure tecniche ed organizzative che assicurano un'adeguata sicurezza dei dati personali, sia che si tratti di dati tenuti in forma cartacea, sia in forma elettronica o elaborati dai sistemi dell'azienda. Ciò include una revisione delle metodologie per testare la sicurezza e delle certificazioni, standard o codici di pratica per la sicurezza informatica.

10. Diritti degli interessati

L'organizzazione ha bisogno di processi che consentano di facilitare e di rispondere agli interessati che esercitano uno o più diritti, incluso il diritto di accesso.