GDPR 30 OTTOBRE 2020

# Garante privacy, il nuovo piano ispettivo: quali lezioni trarre per le aziende

**Federica Lamoratta**
Avvocato, Pirola Pennuto Zei & Associati

**Mario Valentini**
Avvocato e DPO, Pirola Pennuto Zei & Associati

Il piano ispettivo del Garante privacy per il secondo semestre 2020 mira ad accertare soprattutto la presenza e l'accuratezza di policy e procedure contro i data breach: è dunque importante che le aziende siano in grado di dimostrare la propria accountability sia dal punto di vista delle politiche e dei regolamenti aziendali, sia dal punto di vista implementativo e tecnologico. Ecco alcuni utili consigli pratici Con il Provvedimento n. 171 del primo ottobre 2020 l'Autorità Garante privacy ("Garante" o "Autorità") ha deliberato il piano ispettivo per il secondo semestre 2020 (luglio 2020 – dicembre 2020), definendo le priorità in relazione alle risorse disponibili, nonché ha individuato principi e criteri dell'attività ispettiva.

L'attività di accertamento verrà svolta in collaborazione con il Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza, alla luce di quanto disposto nel Protocollo d'intesa del 10 marzo 2016 relativo ai rapporti di collaborazione tra il Garante e la Guardia di Finanza, che consolida le sinergie operative sviluppate tra le due istituzioni e ricomprende l'accertamento in loco, effettuato dal personale dell'Ufficio o delegato alla Guardia di Finanza nei luoghi dove si effettuano i trattamenti di dati, o nei quali occorre effettuare rilevazioni utili al medesimo controllo, nei confronti di soggetti non necessariamente individuati sulla base di reclami o segnalazioni.

## Indice degli argomenti

## Piano ispettivo del Garante privacy: gli ambiti di controllo.

La delibera illustra gli ambiti del controllo e gli obiettivi numerici da conseguire e tiene conto dei procedimenti ispettivi e sanzionatori in corso, nonché di quelli avviati sulla base della precedente programmazione e non ancora conclusi.

Il Garante evidenzia che le attività di ispezione saranno indirizzate agli accertamenti in riferimento a profili di interesse generale per categorie di interessati nell'ambito di molteplici

trattamenti ed illustra che le ispezioni riguarderanno sia il settore pubblico che il settore privato.

L'attività di accertamento, condotta dall'Autorità, prosegue quella avviata nel primo semestre, in quanto è possibile notare una certa linea di continuità rispetto al piano ispettivo del periodo gennaio-giugno 2020, curato dall'ultimo Collegio presieduto da Antonello Soro.

Infatti, l'attenzione dell'Autorità continuerà a interessare aree cruciali per la privacy, quali:

- trattamenti dei dati personali effettuati mediante applicativi per la gestione delle segnalazioni di condotte illecite (c.d. whistleblowing);
- trattamenti dei dati personali effettuati da intermediari per la fatturazione elettronica;
- trattamenti di dati personali effettuati da Enti pubblici in tema di rilascio di certificati anagrafici e di stato civile, attraverso l'accesso ad ANPR;
- trattamenti di dati personali effettuati da società rientranti nel settore denominato "Food Delivery";
- trattamento di dati personali effettuati da società private di rating reputazionale, ovvero da società private in tema di banche reputazionali;
- trattamenti di dati personali effettuati da società private ed Enti pubblici per la gestione e la registrazione delle telefonate nell'ambito del servizio di call center;
- nonché le violazioni della sicurezza dei dati (data breach).

Il Garante evidenzia al riguardo che le ispezioni programmate si focalizzano su alcuni aspetti specifici, quali i controlli nei confronti di soggetti, pubblici e privati, appartenenti a categorie omogenee per quanto riguarda i presupposti di liceità del trattamento e le condizioni per il consenso, qualora il trattamento sia basato su tale presupposto; sul rispetto dell'obbligo dell'informativa, nonché sulla durata della conservazione dei dati.

Il Garante rappresenta che sarà prestata specifica attenzione a profili sostanziali del trattamento che spiegano significativi effetti sugli interessati.

Infatti, nella Newsletter del 26/10/2020 il Garante evidenzia che "*I controlli si concentreranno anche sull'adozione delle misure di sicurezza da parte di pubbliche amministrazioni e di imprese che trattano particolari categorie di dati personali; sul rispetto delle norme sulla informativa e il consenso; sui tempi di conservazione dei dati. L'attività ispettiva verrà svolta anche a seguito di segnalazioni e reclami, con particolare attenzione alle violazioni più gravi*".

Il suddetto provvedimento, inoltre, specifica che l'attività ispettiva programmata riguarderà n. 30 accertamenti ispettivi di iniziativa, effettuati anche a mezzo della Guardia di Finanza, e che l'Ufficio potrà svolgere ulteriori attività ispettive e di revisione d'ufficio ovvero in relazione a segnalazioni o reclami proposti.

Il Garante evidenzia, altresì, che l'Ufficio informerà il Collegio sull'individuazione dei soggetti sottoposti ad ispezione e riferirà, alla fine del semestre, sull'andamento delle attività ispettive e delle attività istruttorie a carattere ispettivo, a qualunque titolo compiute, ai sensi di quanto previsto dall'art. 9, comma 4, lettera e) del Regolamento n. 1/2000, come modificato dalla deliberazione n. 374 del 25 giugno 2015.

Nella Newsletter il Garante sottolinea che il bilancio dell'attività ispettiva e sanzionatoria dell'Autorità nel primo semestre del 2020 registra intanto un notevole incremento delle entrate complessive derivanti dalle sanzioni che passano da 1 milione 223mila euro del primo semestre del 2019 a 7 milioni 108 mila euro, con un aumento del 481%.

Sono state effettuate, altresì, iscrizioni a ruolo per un importo complessivo di 5 milioni 42mila euro (+124%) a fronte dei 2 milioni 248mila euro del primo semestre 2019, che hanno riguardato trasgressori che non si sono avvalsi della facoltà di definizione agevolata prevista dal decreto legislativo n.101 del 2018.

## Rivedere e aggiornare le policy privacy aziendali in ottica accountability

Alla luce del sopra menzionato piano di ispezioni e in considerazione delle sanzioni irrogate alle organizzazioni, soprattutto aziendali, risulta, quindi, imprescindibile per queste ultime rivedere e aggiornare le proprie policy, inerenti alla gestione del trattamento dei dati personali di cui sono in possesso, tra cui quelle disposte in materia di data breach.

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

Ciò che viene richiesto al Titolare del trattamento ("Titolare") in sede ispettiva è comprovare la propria accountability, ovvero l'attuazione di misure tecniche e organizzative opportune, efficaci e adeguate per la salvaguardia dei dati personali trattati.

Questo significa 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 operate.

L'importanza dell'accountability emerge, infatti, in fase di controllo del Garante dove l'azienda dovrà dimostrare agli ispettori, con ragionamento logico e documentato, quanto ha fatto concretamente per adempiere alla normativa GDPR ed eventualmente difendersi da scelte opinabili, quali ad esempio il non aver nominato un Data Protection Officer ("DPO") o non aver predisposto il registro dei trattamenti ex art. 30 GDPR.

Al termine dell'ispezione l'organizzazione potrà valutare se si sta agendo in modo adeguato al GDPR o se si stanno trascurando azioni importanti.

Inoltre, durante l'attività ispettiva è necessario dimostrare l'applicazione della normativa, fornendo evidenza dei processi in atto. È opportuno, quindi, non farsi cogliere impreparati e individuare ex ante i soggetti preposti alla gestione degli ispettori.

Inoltre, è fondamentale per le aziende dotarsi di una procedura di gestione dell'ispezione, effettuate da tali Autorità. Tale documento costituisce uno strumento per dimostrare la propria accountability, contenente le procedure, i ruoli e i comportamenti da seguire in caso di ispezione dell'Autorità o della Guardia di Finanza. In caso di ispezione da parte delle Autorità, è sempre opportuno per l'azienda avere un atteggiamento collaborativo con le stesse.

Tale atteggiamento collaborativo implica l'obbligo di fornire l'accesso a documenti cartacei e in formato elettronico contenuti nei pc, hard disk, nonché in ogni altro dispositivo informatico.

Inoltre, implica per l'azienda l'obbligo di indicare dove sono conservati i documenti d'interesse e l'obbligo di fornire ogni informazione richiesta dagli ispettori, indipendentemente dal fatto che le informazioni o i documenti siano tenuti in luoghi diversi o da soggetti diversi dal Titolare del trattamento, quali responsabili del trattamento.

## Come avviene l'attività ispettiva del Garante

Le ispezioni, inoltre, vanno ben gestite da un punto di vista emotivo e vanno preparate adeguatamente e professionalmente: pertanto, il Titolare del trattamento dovrà porsi sempre come un punto di riferimento, dimostrare di essere preparati e pronti alle domande che possono essere fatte.
Al riguardo il Titolare dovrà rilasciare dichiarazioni o affermare solo ciò che può provare.

Inoltre, il Titolare dovrà evitare di dichiarare il falso o di omettere volutamente le informazioni che vengono richieste.

Con riguardo alle modalità di conduzione dell'ispezione, gli ispettori possono accedere agli uffici o luoghi dove deve essere svolta l'ispezione dalle 07.00 alle 20.00 e può mediamente durare due o tre giorni.

L'accertamento può avvenire "a sorpresa" o anticipato al Titolare del trattamento il giorno prima tramite PEC o telefonata, in modo che possa farsi trovare presente all'appuntamento, eventualmente con il DPO, ove presente.

I funzionari dell'Autorità possono richiedere ogni documento e/o informazione oggetto della verifica. Gli stessi possono anche apporre i sigilli su database e documenti.

Inoltre, gli ispettori possono svolgere interrogatori ai quali occorre rispondere in modo corretto, chiaro e non evasivo e far riferimento il più possibile alle procedure adottate. Al riguardo, il Titolare deve evitare di fornire risposte generiche e, piuttosto che rilasciare dichiarazioni che non possono essere provate, può riservarsi di fornire, anche successivamente, chiarimenti e/o risposte, nonché documentazione più dettagliata.

I funzionari dell'Autorità non possono, tuttavia, cercare documenti che non hanno alcun collegamento con l'oggetto dell'ispezione o richiedere e pretendere l'originale dei documenti, in quanto il Titolare dovrà sempre consegnare soltanto copie dei documenti e degli atti oggetto dell'ispezione.

Inoltre, non possono effettuare interviste e svolgere domande non pertinenti, né rilevanti per l'oggetto dell'ispezione. Eventuali informazioni assunte, che esulino dall'oggetto dell'indagine, potranno essere debitamente impugnate con le modalità consentite dalla legge.

Al termine dell'attività ispettiva viene verbalizzato quanto emerso. Se ritenuto opportuno, è possibile richiedere di mettere a verbale dichiarazioni di cui si desidera lasciare traccia. In caso di dubbio, è fondamentale, inoltre, per il Titolare 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.

È, quindi, opportuno 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, nonché rilasciare solo copie e mai documentazione in originale.

## Una check-list di accountability da usare durante l'ispezione

Con riferimento alle fasi dell'ispezione, all'avvio dell'ispezione, i soggetti preposti alla gestione degli ispettori, dovranno coinvolgere il DPO, ove nominato, e/o il legale di riferimento.

Inoltre, occorrerà per il Titolare aver predisposto, precedentemente, una check-list di accountability, che elenchi tutta la documentazione, le procedure, i processi e le misure di sicurezza adottate all'interno della realtà aziendale.

Infatti, in un'ottica di accountability occorre elencare tutte le misure organizzative e tecniche adottate all'interno della realtà aziendale, nonché creare flussi interni per la raccolta evidenze (attività svolte dal DPO, audit privacy svolti presso l'azienda, esercizio dei diritti degli interessati, tenuta dei vari registri, raccolta dei consensi, procedura e registro data breach).

Infatti, durante l'ispezione vengono tipicamente richiesti al Titolare i seguenti documenti:

- 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 è il registro dei trattamenti di cui all'art. 30 GDPR. Tale documento deve contenere l'inventario di tutti i trattamenti di dati personali eseguiti dall'azienda ed è considerato indice di una corretta gestione dei trattamenti. Proprio per questo, 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 sul trattamento dei dati personali ex artt. 13 e 14 GDPR, adottate dall'organizzazione.

Dal registro, quindi, sarà possibile disegnare una mappa immediata dei flussi di dati in entrata e in uscita, dei relativi responsabili, oltreché delle misure di sicurezza adottate.

Inoltre, in base poi al processo dichiarato, se ne valuterà la gestione, anche dal lato informatico.

L'Autorità, inoltre, procederà poi ad effettuare ulteriori controlli fra cui, se prevista, la nomina del DPO in relazione agli artt. 37 e ss. GDPR, e la verifica delle nomine dei responsabili ex art. 28 GDPR e, in particolare, la verifica delle relative istruzioni sul trattamento impartite dal Titolare mediante contratti o atti giuridici, con acquisizione degli stessi, che il Titolare dovrà mettere a disposizione in copia.

## Piano ispettivo del Garante privacy: DPO, informative e data retention

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

Il mero conferimento dell'incarico ad un DPO non è di per sé sufficiente a dimostrare la conformità da parte dell'azienda al GDPR.

In sede di ispezione, l'Autorità chiederà di produrre la nomina formale del DPO, la comunicazione della stessa al Garante, i verbali delle riunioni svolte con il DPO e i report interni effettuati a quest'ultimo dai referenti privacy.

Inoltre, è opportuno evidenziare che le Autorità 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.

Fondamentale, inoltre, deve essere l'attenzione concreta del Titolare ai processi d'istruzione dei soggetti che trattano quotidianamente i dati. La verifica della formazione privacy, erogata al personale autorizzato al trattamento dei dati, è un aspetto essenziale per evidenziare l'accountability del Titolare e costituente una misura di sicurezza, oltreché un diritto e dovere per dipendenti e collaboratori.

Infatti, sono numerose le volte in cui il Garante, in sede ispettiva, 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 o in tema di videosorveglianza), verificando la reale preparazione del personale addetto.

Altro elemento imprescindibile è avere le informative di cui agli artt. 13 e 14 GDPR in regola, in modo da 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.

Con riguardo, invece, alla gestione dei tempi di conservazione dei dati, è opportuno definire il tempo di conservazione di un dato valutando la finalità del trattamento nel quale è coinvolto. Pertanto, 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.

È opportuno, quindi, per il Titolare effettuare a monte un'esaustiva mappatura dei dati personali trattati, oltreché dei vari supporti di conservazione, al fine di garantire una corretta e coerente gestione della data retention. Solo definendo preventivamente una policy sulle modalità di archiviazione dei dati, sarà possibile in fase di controllo comprovare una corretta e reale gestione dei tempi di conservazione.

## DPIA e procedure contro i data breach: aree cruciali delle ispezioni

Inoltre, gli ispettori richiederanno la valutazione d'impatto (DPIA) o il fondamento delle ragioni che ne hanno escluso l'adozione; occorre, quindi, per il Titolare individuare 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, geolocalizzazione 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.

Infine, uno dei motivi principali da cui potrebbe derivare un'ispezione da parte del Garante è la mancata notifica di una violazione dei dati personali (data breach) alla stessa Autorità, di cui ne sia venuta comunque a conoscenza, ad esempio tramite un reclamo presentato alla suddetta Autorità, o l'avvenuta notifica di un data breach su cui il Garante intenda ottenere maggiori informazioni.

In tasi ipotesi, quindi, il Titolare deve assicurarsi che ci sia una procedura interna su come gestire le violazioni dei dati personali e che tale procedura preveda anche gli obblighi cui sono tenuti i fornitori di servizi eventualmente coinvolti dalla violazione dei dati personali.

Al riguardo, è utile che il Titolare, al fine di non incorrere in sanzioni, predisponga un'attività di formazione in tema di data breach. Spesso, infatti, le violazioni non sono notificate all'Autorità, in quanto il personale non sempre è in grado di comprendere se un determinato comportamento costituisca violazione dei dati personali.

In altri casi, invece, alcune aziende preferiscono non effettuare la notifica, al fine di evitare possibili indagini da parte dell'Autorità.

Siffatte azioni non risultano conformi con quanto richiesto dalla normativa e, pertanto, risulta necessaria la predisposizione da parte del Titolare di un'attività di formazione in tema di data breach.

Adottare politiche di protezione, che consistano non solo nel decidere in 72 ore “se notificare”, ma che prevedano 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 della violazione dei dati personali, si configura da parte del Titolare dimostrazione di accountability.

Inoltre, è opportuno che il Titolare proceda con l’adozione di un protocollo di risposta, che dovrà essere verificato periodicamente per controllarne la validità.

È utile, inoltre, che il Titolare si doti di una copertura assicurativa per eventuali data breach, di un registro dei casi di data breach, ed, infine, che compia un’attività di indagine volta ad individuare la natura e la portata della violazione.

Infine, è importante per il Titolare dare dimostrazione dell’attuazione delle misure tecniche di cui all’art. 32 GDPR, ovvero:

- l’eventuale pseudonimizzazione e cifratura dei dati personali;
- la capacità di assicurare la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi del trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico;
- l’adozione di una procedura per testare, verificare e valutare l’efficacia delle misure tecniche ed organizzative, finalizzate a garantire la sicurezza del trattamento.

In particolare, il Titolare dovrà indicare tutte le misure adottate per accedere alle banche dati o alle varie cartelle presenti (username e password – modalità di autenticazione), i backup effettuati e le modalità con cui vengono effettuati, gli antivirus presenti, nonché gli eventuali alert implementati sui sistemi.

A tal fine, il Titolare sarebbe dovrebbe acquisire dall’amministratore di sistema e/o dal responsabile esterno del trattamento una relazione sullo stato dei sistemi (gap analysis), nonché un piano di implementazione sulle misure da attuare.

## Piano ispettivo del Garante privacy: consigli per le aziende

In conclusione, al fine di non incorrere nelle sanzioni comminate dall’Autorità a seguito dell’effettuazione dell’attività ispettiva, è necessario, che le aziende facciano tesoro dei provvedimenti finora disposti dall’Autorità.

È necessario, altresì, che facciano proprio il principio di accountability, avendo, quindi, la consapevolezza della necessità di giustificare ogni scelta e decisione compiuta.

Inoltre, è necessario che si adeguino alle migliori prassi operative e di sicurezza, e che adottino i provvedimenti più idonei ed opportuni al fine di ottemperare a quanto disposto nel GDPR, sia dal punto di vista delle politiche e dei regolamenti aziendali, sia dal punto di vista implementativo e tecnologico, fornendo sessioni formative per i soggetti, operanti all’interno delle predette organizzazioni, che trattano quotidianamente i dati personali.

È questa la migliore lezione che, tenendo conto delle prossime attività ispettive, i titolari dei trattamenti possono trarre da quello che, in passato, è accaduto durante le verifiche dell'Autorità.