



REGOLAMENTO (UE) 2016/679 E ATTIVITA' ISPETTIVE DEL GARANTE PRIVACY

Incontro del 20/05/2023 Presso Sede dell'Ordine Periti e Periti Industriali di Vicenza

SOMMARIO

1. Regolamento (UE) 2016/679: Chi effettua i controlli
2. Tipologie di controlli
3. Campagna Controlli Gennaio-Giugno 2023
4. Quadro sanzionatorio: sanzioni amministrative e penali



1. REGOLAMENTO (UE) 2016/679: CHI EFFETTUA I CONTROLLI

Il garante della privacy può intervenire direttamente con il suo personale o con il Corpo Ispettivo dedicato:

- Nucleo speciale tutela privacy e Frodi Tecnologiche (NSTPFT): ispettori specializzati sulle tematiche privacy;
- Guardia di Finanza.

Attività Ispettive previste:

- Il reperimento di dati ed informazioni sui soggetti da controllare;
- L'assistenza nei rapporti con le autorità giudiziarie;
- La partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e altre rilevazioni dei luoghi ove si svolge il trattamento;
- Lo sviluppo delle attività delegate o sub-delegate per l'accertamento delle violazioni di natura penale o amministrativa;
- La contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;
- L'esecuzione d'indagini conoscitive sullo stato di attuazione del regolamento in settori specifici;
- La segnalazione all'autorità di tutte le situazioni rilevanti ai fini dell'applicazione del codice, di cui venga a conoscenza nel corso dell'esecuzione delle ordinarie attività di servizio.

2. TIPOLOGIE DI CONTROLLI

I controlli effettuati dai soggetti autorizzati possono essere:

- Su attività ispettiva programmata (campagne dedicate);
- Verifiche a sorpresa su una serie di soggetti identificati a priori;
- Accessi per raccolta informazioni.

Su segnalazione, reclamo:

- Accesso o richiesta scritta per raccolta informazioni;
- Provvedimento esecutivo a seguito di istruttoria;
- Non necessariamente sfociano in un controllo se è una segnalazione è anonima.

Chi può effettuare la segnalazione ? Cittadini, Clienti, Iscritti, Dipendenti, ecc..



3. CAMPAGNA DI CONTROLLO GENNAIO-GIUGNO 2023

Deliberazione del 26 gennaio 2023 - Attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo Gennaio-Giugno 2023 [9862660]

Registro dei provvedimenti

n. 23 del 26 gennaio 2023

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERA

limitatamente al periodo gennaio/giugno 2023, l'attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, è indirizzata:

a) in via prioritaria, al completamento delle attività ispettive già iniziate nel corso del secondo semestre dell'anno 2022 con particolare riguardo a:

a1) verifiche sui gestori dell'identità digitale e sui fornitori di servizi che utilizzano SPID e CIE (anche ad uso professionale o per minori) nell'ambito di servizi online offerti anche mediante APP da parte delle pubbliche amministrazioni;

a2) verifiche in ordine alla corretta implementazione delle Linee guida sui cookie e gli altri strumenti di tracciamento anche attraverso lo strumento degli accertamenti online;

a3) prosecuzione delle verifiche in materia di trattamento di dati personali attraverso attività di telemarketing e tessere di fidelizzazione.

b) Altri accertamenti nei confronti di soggetti pubblici e privati, al fine di verificare l'osservanza delle disposizioni in materia di protezione dei dati personali, ivi incluse le istruttorie relative a reclami e segnalazioni formali proposti all'Autorità ed in istruttoria presso i relativi Dipartimenti e Servizi.

L'attività ispettiva programmata con la deliberazione in data odierna riguarderà, relativamente ai punti a) e b) n. 60 accertamenti ispettivi in loco di iniziativa, effettuati anche a mezzo della Guardia di finanza.

Resta fermo che l'Ufficio potrà svolgere ulteriori attività istruttorie di carattere ispettivo d'ufficio, o in relazione a segnalazioni o reclami proposti.

L'Ufficio informerà mensilmente il Collegio sui soggetti ispezionati appartenenti alle categorie a) e b) e riferirà, alla fine del semestre, sull'andamento complessivo 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).

Roma, 26 gennaio 2023 IL PRESIDENTE

Stanzione



SI TRATTA DI UN'ISPEZIONE SOSTANZIALE

- Verifica della coincidenza tra quanto dichiarato formalmente e quanto effettivamente esistente e/o operativo (es. conservazione dati, consenso, ecc);
- Accountability, non solo corresponsabilizzazione nelle decisioni, ma anche capacità di dimostrare quanto dichiarato;
- Il controllo prevede un accesso da parte di un gruppo (minimo due persone) di finanziari del nucleo privacy;
- Il controllo prevede un foglio di raccolta di informazioni in merito ad un elenco di punti;
- Il controllo richiede di descrivere alcune attività inerenti la richiesta di informazioni;
- Il controllo richiede di esibire documenti ed evidenze.

L'esito del controllo è un verbale: risposta ai punti di richiesta informazioni ed allegati con le evidenze.

COSA FARE IN UN CONTROLLO

- Contattare il referente privacy aziendale o il D.P.O. che deve coordinare l'attività;
- Verificare il foglio di richiesta informazioni;
- Valutare se necessario un supporto legale;
- Fornire risposte concise e circoscritte all'oggetto dell'ispezione;
- Se non sia certezza della risposta, riservarsi di fornire una risposta scritta successivamente;
- Mostrare solo i documenti relativi per ispezione, fornendoli in copia e non in originale;
- Verificare sempre quanto verbalizzato dagli ispettori;
- Se un'attività ispezionata non è idonea, definire subito un piano di azioni correttive e presentarlo.

4. QUADRO SANZIONATORIO: CAMPAGNA CONTROLLI GENNAIO-GIUGNO 2023

Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

- Fino a 10 milioni o al 2% del fatturato mondiale (se superiore);
- Fino a 20 milioni o al 4% del fatturato mondiale (se superiore).

SANZIONI PECUNIARIE: SOGLIE

Max 10 milioni di euro (fino al 2% del fatturato se superiore a 10 milioni) nei seguenti casi:

- Mancato Consenso per minori;
- Misure di sicurezza non adeguate;
- Accountability;
- Principi di Privacy by Design e By Default;
- Adempimenti in generale del Titolare del Responsabile e del Rappresentante;
- Non adeguata Gestione Data Breach;
- Mancata Notifica al garante privacy;
- Valutazione di impatto non adeguata;
- Mancata identificazione Responsabile per la protezione dei dati.



Max 20 milioni di euro (fino al 4% del fatturato se superiore a 10 milioni) nei seguenti casi:

- Mancata definizione Regole per la raccolta e documentazione del consenso;
- Non rispetto dei Principi di correttezza e liceità dei trattamenti;
- Mancata gestione dei Diritti degli interessati;
- Trasferimenti di dati extra Ue non informati;
- Ordini emessi dal garante privacy;
- Data Breach comunicazione agli interessati;
- Rispetto a specifici divieti di trattamenti;
- Rispetto obblighi per specifici casi (esempio dati dei lavoratori nel contesto del rapporto di lavoro, ecc.).

SANZIONI PENALE

Rappresentate nell'art. 167 e 167 Bis, Ter del D.Lgs. 196/2003 aggiornato dal D.Lgs. 101/2018.

- Art. 167 - trattamento illecito di dati (trarre profitto per sé a danno degli interessati): reclusione da 6 mesi a un 1 e 6 mesi; da 1 a 3 anni.
- Art.167 Bis - comunicazione e diffusione illecita di dati personali (trarre profitto per sé a danno degli interessati) reclusione da 1 a 6 anni.
- Art. 167 Ter - Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (trarre profitto per sé a danno dell'interessati): reclusione da 1 a 6 anni.
- Art. 168 - Falsità nelle dichiarazioni al Garante ed interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri da parte del Garante: reclusione da 6 mesi a 3 anni.
- Art. 170 - inosservanza del provvedimento del Garante: reclusione da 3 mesi a 2 anni.

PROVVEDIMENTI

Non necessariamente i controlli generano sanzioni ma potrebbero generare anche:

- Provvedimenti con indicazione di blocco del trattamento;
- Misure di contrasto all'illecito;
- Richiesta di maggiori dettagli o richieste di maggiori misure di sicurezza.

Grazie dell'Attenzione