



Formazione privacy, antiriciclaggio e sicurezza dati digitali

Modulo III/V

www.conepro.it

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Carta dei diritti fondamentali dell'Unione Europea

“ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano” e che “tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge”.

Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente, che in Italia è individuata nel Garante per la protezione dei dati personali.

Art. 47 della Carta si preoccupa di garantire l'attuazione del diritto alla protezione dei dati personali sancendo che ciascun cittadino ha diritto ad un ricorso effettivo innanzi a un giudice.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196), come modificato dal Decreto legislativo 10 agosto 2018, n. 101.

Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51)

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Strumenti di tutela amministrativa e giurisdizionale nel GDPR

Il Regolamento europeo 679/2016 disciplina gli strumenti di tutela amministrativa e giurisdizionale agli artt. 77 e ss. prevedendo:

- 1) La tutela in via amministrativa innanzi all'autorità di controllo (Garante) rispetto ad un trattamento dei propri dati effettuato in violazione del regolamento;
- 2) La tutela in via giurisdizionale relativa ai provvedimenti e ad ogni decisione giuridicamente vincolante dell'autorità di controllo (Garante)
- 3) La tutela in via giurisdizionale innanzi al giudice ordinario volta a fare valere un proprio diritto riconosciuto dal Regolamento nei confronti di chi ha effettuato il trattamento

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Alternatività degli strumenti

Il D. Lgs n. 101/2018 è intervenuto sul Codice Privacy 196/2003, in riferimento alle tutele amministrative e giurisdizionali già esistenti.

L'art. 140 bis del Codice sancisce il principio dell'alternatività degli strumenti di tutela. Per cui l'interessato che ritenga violato uno o più diritti relativi ai propri dati personali può scegliere se:

- 1) adire in via amministrativa l'autorità di controllo competente oppure
- 2) proporre ricorso innanzi all'autorità giudiziaria ordinaria

Resta salva la possibilità di adire l'autorità giudiziaria avverso i provvedimenti vincolanti del Garante ovvero in caso di inerzia del Garante (qualora il reclamo non venga deciso entro 9 mesi dal garante ovvero se il garante ometta di informare l'interessato trascorsi tre mesi della proposizione del reclamo).

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Segnalazioni al Garante

Chiunque può scegliere di inviare al Garante una "segnalazione" (ai sensi dell'articolo 144 del Codice privacy), quando non è possibile presentare un reclamo circostanziato, non disponendosi di sufficienti informazioni, oppure qualora si preferisca effettuare una sorta di "denuncia" che possa spingere il Garante ad effettuare un controllo sull'attività asseritamente illecita di un Titolare del trattamento o sull'eventuale violazione della normativa.

La segnalazione può essere esaminata dall'Autorità, ma non comporta la necessaria adozione di un provvedimento.

Il dipartimento, servizio o altra unità organizzativa competente può concludere l'esame della segnalazione disponendone l'archiviazione ad esempio in caso di segnalazioni del tutto generiche.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Il Reclamo al Garante

Il reclamo è lo strumento che consente all'interessato di rivolgersi al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali (art. 77 del Regolamento Ue 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento) e di richiedere una verifica dell'Autorità.

Il reclamo può essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione senza scopo di lucro. In tali casi, è necessario conferire una procura da depositarsi presso il Garante assieme a tutta la documentazione utile e un recapito per l'invio di comunicazioni anche tramite posta elettronica, fax o telefono.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Come si presenta il Reclamo

Il reclamante potrà far pervenire l'atto utilizzando la modalità ritenuta più opportuna, consegnandolo a mano presso gli uffici del Garante (all'indirizzo di seguito indicato) o mediante l'inoltro di:

a) raccomandata A/R indirizzata a: Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 Roma

b) messaggio di posta elettronica certificata indirizzata a: protocollo@pec.gpdp.it

Il reclamo al Garante deve contenere 1) indicazione per quanto possibile dettagliata dei fatti; 2) delle circostanze su cui si fonda; 3) delle disposizioni che si presumono violate, delle misure richieste;

4) gli estremi identificativi del Titolare o del Responsabile del trattamento, ove conosciuto.

Segue un istruttoria preliminare e all'esito, quando il reclamo non viene archiviato, viene avviato il procedimento.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Il Reclamo al Garante: procedimento

Qualora l'istante non abbia preventivamente esercitato i diritti di cui agli articoli da 15 a 22 del RGPD con istanza rivolta al titolare del trattamento, se dal reclamo non emergano specifiche e fondate ragioni che ne giustifichino la mancata effettuazione, il dipartimento, servizio o altra unità organizzativa ai quali il reclamo è assegnato invita, entro quarantacinque giorni dalla data della ricezione del reclamo, l'istante a rivolgersi al titolare del trattamento.

All'esito del procedimento, durante il quale il reclamato può chiedere di essere sentito con audizione e può presentare deduzioni scritte e documenti, il Collegio del Garante provvede con propria deliberazione e adotta, ove necessario, i provvedimenti correttivi e sanzionatori di cui all'articolo 58, paragrafo 2, del GDPR. Il Collegio provvede con propria deliberazione anche quando rileva l'infondatezza del reclamo.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

I poteri «correttivi»

Ad esito del procedimento, e anche prima dell'istruttoria, il Garante può esercitare i propri poteri correttivi individuando le misure.

I poteri «correttivi» nel Regolamento sono stabiliti all'art. art. 58, c. 2 del Regolamento quali ad esempio:

- 1) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale;
- 2) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- 3) ingiungere al titolare o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i loro diritti.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

I poteri ispettivi del Garante

Nell'esercizio dei compiti di controllo o comunque esercitabili dal Garante, valutati gli elementi in suo possesso e anche in assenza di reclamo, segnalazione o notificazione di violazione dei dati personali, l'Autorità può avviare d'ufficio un'istruttoria preliminare per verificare la sussistenza di idonei elementi in ordine a possibili violazioni della disciplina rilevante in materia di protezione dei dati personali

Le ispezioni sono effettuate sulla base di programmi elaborati secondo linee di indirizzo stabilite dal Garante che individua i titolari dei trattamenti da sottoporre a controllo.

Tra i poteri ispettivi vi sono quelli di:

- ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti
- ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

I poteri ispettivi del Garante

Qualora gli accertamenti siano svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali (art. 158, c. 3)

Guardia di Finanza: Nucleo Speciale Tutela Privacy e Frodi Tecnologiche

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Ricorso all'autorità giudiziaria (avverso una decisione del Garante)

Concluso il procedimento davanti al garante sia con un'archiviazione che con un'ingiunzione ai sensi dell'art. 78 del Regolamento è possibile proporre ricorso giurisdizionale avverso una decisione giuridicamente vincolante dell'autorità di controllo ed in particolare avverso:

- a) i provvedimenti prescrittivi di rigetto o archiviazione adottati a seguito di reclami
- b) i provvedimenti prescrittivi e le ordinanze ingiunzione adottati a seguito di procedimenti di contestazione di violazioni amministrative.

L'art. 78 comma 2 del Regolamento prevede altresì la facoltà di proporre ricorso qualora l'autorità di controllo non tratti un reclamo nei termini normativamente stabiliti o non informi l'interessato sullo stato del reclamo nel termine di tre mesi.

Il ricorso e il decreto di fissazione dell'udienza devono essere notificati anche al garante.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Ricorso all'autorità giudiziaria e risarcimento del danno

Il ricorso al Garante presenta ad oggi significativi vantaggi essendo celere e con costi molto contenuti. Tuttavia il Garante non ha la potestà per pronunciarsi in ordine ai profili risarcitori della violazione per cui l'interessato dovrà in ogni caso adire l'autorità giudiziaria ordinaria per ottenere la liquidazione dell'eventuale danno da illecito trattamento dei propri dati personali.

L'art. 152 del Codice novellato disciplina le controversie concernenti la normativa in materia di protezione dei dati personali nonché il diritto al risarcimento del danno da illecito trattamento degli stessi e rinvia per la disciplina del procedimento all'art. 10 del D.lgs. 150/2011.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Ricorso all'autorità giudiziaria e risarcimento del danno il procedimento

La competenza è alternativamente quella del tribunale del luogo in cui risiede l'interessato o quella del luogo ove il titolare del trattamento ha la propria sede o risiede.

Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante affinché possa presentare osservazioni

L'efficacia esecutiva del provvedimento impugnato può essere sospesa quando ricorrano gravi e circostanziate ragioni.

La sentenza che definisce il giudizio non è appellabile, ma sempre impugnabile per Cassazione e può prescrivere le misure coercitive per consentire l'adempimento.

Formazione privacy, antiriciclaggio e sicurezza dati digitali

Il danno risarcibile patrimoniale e non patrimoniale

Il GDPR afferma il diritto dell'interessato, quando danneggiato, di ottenere il risarcimento del danno subito, che potrà essere sia patrimoniale (materiale) che non patrimoniale (immateriale).

Il d.lgs. 101/2018 ha abrogato l'art. 15 d.lgs. 196/2003 in base al quale il legislatore aveva previsto che "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile".

Ad oggi la norma di riferimento – avente natura sostanziale è unicamente l'art. 82 del Regolamento il quale prevede che il Titolare e Responsabile possano liberarsi provando che il danno non è a loro imputabile .

Formazione privacy, antiriciclaggio e sicurezza dati digitali

L'imputabilità del danno e l'esenzione da responsabilità

Il Titolare del trattamento ed il Responsabile del Trattamento rispondono in via solidale del danno.

Il Titolare e il Responsabile del trattamento (o il Contitolare) vanno esenti da responsabilità se dimostrano che l'evento dannoso non è in alcun modo a loro imputabile (Art. 82, par. 3 - inversione dell'onere della prova).

Il Titolare, Il Contitolare o il Responsabile del trattamento dovranno poter provare, alternativamente, che l'evento dannoso non è loro ascrivibile in quanto dipendente da una fonte estranea alla loro sfera di competenza o di controllo, oppure che sono state da loro predisposte - in seguito alla valutazione dei rischi - ed attuate tutte le prevedibili misure adeguate (Art. 32 GDPR) al fine di evitare che si verificasse il danno.



GRAZIE PER L'ATTENZIONE

AVV. ELENA IEMBO

VIA PO', 22 - ROMA

3470320758