CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SESSIONE FORMATIVA ON LINE CORSO DI PERFEZIONAMENTO

Come gestire una visita ispettiva

Autore Dott.ssa Gloriamaria Paci

Studio Paci & C. Srl
Studio Consulenza Privacy Dott.ssa Gloriamaria Paci
Via Edelweiss Rodriguez Senior, 13
47924 Rimini (Rn)

Telefono: 0541 – 1795431
Telefax: 0541 - 1794118
Cellulare: 347-5244264
Mail: info@consulenzepaci.it
Sito web: www.consulenzepaci.it

Seguici sui social!
https://linktr.ee/studiopaci

Associazione Protezione Diritti e Libertà Privacy APS
Via Edelweiss Rodriguez Senior, 13
47924 Rimini (Rn)
Tel. 0541-1795431 / Fax 0541-1794118
Cell. Gloriamaria Paci 347-5244264

segreteria@associazionedirittiprivacy.it
posta@pec.associazionedirittiprivacy.it
www.associazionedirittiprivacy.it

Seguici sui social!

https://lintr.ee/apdlp

Gloriamaria Paci

Nata a Rimini nel gennaio del 1969, dopo alcuni anni dedicati alla carta stampata, nel 1998 Gloriamaria decide di scommettere ed investire in un settore allora poco conosciuto: la normativa sulla tutela dei dati personali.

L'esperienza di giornalista pubblicista, affiancata a quella di consulente privacy nel settore pubblico e privato, sia sul territorio italiano che in paesi Extra UE (RSM), verrà impiegata per pubblicare numerosi articoli e testi di settore.

Relatrice a convegni, seminari e corsi di formazione, con l'introduzione del Regolamento Europeo 2016/679, oggi ricopre il ruolo di Responsabile per la protezione di dati personali per privati ed enti pubblici.

Presidente dell'Associazione protezione diritti e libertà privacy, porta avanti progetti ed iniziative finalizzate all'aggregazione di quanti sono interessati alla salvaguardia dei diritti e delle libertà personali nell'ambito della protezione dei dati.

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

Il valore della protezione dei dati personali

«La violenza.
Penso a quella più odiosa sulle donne. Vorrei rivolgermi ai più giovani. Cari ragazzi, ve lo dico con parole semplici: l'amore non è egoismo, dominio, malinteso orgoglio. L'amore – quello vero – è ben più che rispetto: è dono, gratuità, sensibilità. Penso anche alla violenza verbale e alle espressioni di denigrazione e di odio che si presentano, sovente, nella rete. Penso alla violenza che qualche gruppo di giovani sembra coltivare, talvolta come espressione di rabbia".

«Affermare i diritti significa prestare attenzione alle esigenze degli studenti, che vanno aiutati a realizzarsi. Il cui diritto allo studio incontra, nei fatti, ostacoli. A cominciare dai costi di alloggio nelle grandi città universitarie; improponibili per la maggior parte delle famiglie. Significa rendere effettiva la parità tra donne e uomini: nella società, nel lavoro, nel carico delle responsabilità familiari».

Sergio Mattarella - Presidente della Repubblica - messaggio agli italiani – Dicembre 2023

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

"La quantità e la qualità dei dati, la loro velocità possono essere elementi posti al servizio della crescita delle persone e delle comunità. Possono consentire di superare arretratezze e divari, semplificare la vita dei cittadini e modernizzare la nostra società. Occorre compiere scelte adeguate, promuovendo una cultura digitale che garantisca le libertà dei cittadini".

Sergio Mattarella - Presidente della Repubblica - messaggio agli italiani – Dicembre 2022

«I dati servono a guidare il governo del Paese in modo tale da rendere la nostra democrazia più forte abbattendo le disuguaglianze che ancora la indeboliscono, i dati servono a rendere la nostra amministrazione più efficiente e, quindi, a semplificare la vita ai cittadini e i dati servono a portare la nostra società in un presente che strizza l'occhio a un futuro che è già qui, tirandola via dalla atavica arretratezza nella quale decenni di governo dell'innovazione miope l'hanno relegata. I dati, insomma, come la leva con la quale Archimede si dichiarava pronto a sollevare il mondo e noi, con ambizioni non da meno, potremmo risollevare le sorti del nostro Paese».

Avv. Guido Scorza – Componente Autorità Garante per la protezione dei dati personali - *(HuffPost, 2 gennaio 2023)*

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

La protezione dei dati quale riconoscimento di un diritto costituzionalmente garantito

Privacy non significa soltanto diritto di essere lasciati in pace o di proteggere la propria sfera privata

Diritto di controllare l'utilizzo e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione

CONSULENZE PACI PRIVACY

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Associazione Protezione Diritti e Libertà Privacy APS

La protezione dei dati personali è un diritto fondamentale perché tutela la dignità, la libertà, l'identità personale, l'eguaglianza, la non discriminazione, la riservatezza degli individui nei confronti dei soggetti pubblici e privati

Il diritto alla protezione dei dati personali non è solo un diritto ma garanzia di libertà e democrazia

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Si rende ancora più necessaria l'adozione di politiche sulla sicurezza per tutelare i dati di chi si avvale della rete e dei servizi offerti da enti pubblici e privati

Vanno garantiti i canali di trasmissione e la connessione fra le banche dati.

Per raggiungere la compliance al GDPR è fondamentale la collaborazione fra professionisti e la creazione di modelli integrati

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Considerando 4 Regolamento Europeo 2016/679

(4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

La protezione dei dati personali è contemplata dall'articolo 8 della Carta dei diritti dell'Unione Europea

Carta dei diritti dell'Unione Europea

Art. 8 - Protezione dei dati di carattere personale

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. 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. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

I poteri dell'Autorità Garante

POTERI – Articolo 58 Regolamento Europeo 2016/679

Ogni autorità di controllo ha tutti i poteri d'indagine seguenti:

ISPETTIVI

- Condurre indagini
- Richiedere informazioni
- Ottenere, dal titolare 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 e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri

POTERI – Articolo 58 Regolamento Europeo 2016/679

Ogni autorità di controllo ha tutti i poteri d'indagine seguenti:

CORRETTIVI

- Rivolgere avvertimenti al titolare o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del regolamento
- Rivolgere ammonimenti al titolare o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del regolamento
- Ingiungere al titolare o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti derivanti dal regolamento
- Ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una determinata maniera ed entro un determinato termine
- Ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali
- Imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento
- Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali
- Revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono più soddisfatti
- Infliggere una sanzione amministrativa pecuniaria
- Ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale

POTERI – Articolo 58 Regolamento Europeo 2016/679

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Ogni autorità di controllo ha tutti i poteri d'indagine seguenti:

AUTORIZZATIVI E CONSULTIVI

- Fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36 (Valutazione d'impatto)
- Rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali
- Autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato richiede una siffatta autorizzazione preliminare
- Rilasciare un parere sui progetti di codici di condotta e approvarli
- Accreditare gli organismi di certificazione
- Rilasciare certificazioni e approvare i criteri di certificazione
- Adottare le clausole tipo di protezione dei dati
- Autorizzare le clausole contrattuali
- Autorizzare gli accordi amministrativi
- Approvare le norme vincolanti d'impresa

POTERI DELL' AUTORITA'

L'accesso dell'Autorità di controllo non conosce limiti: **«tutti» i dati personali, i locali e i mezzi di trattamento**, nonché «tutte» le informazioni necessarie all'Autorità.

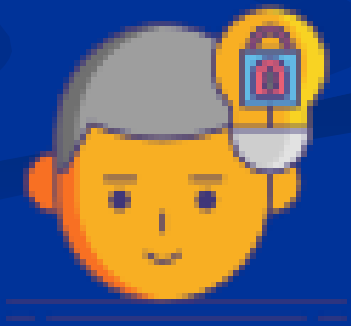
La mancata osservanza di tali disposizioni (quindi anche solo un accesso parziale in assenza di idonee giustificazioni) è qualificata (ai sensi dell'art. 83,l par. 5, lett. e) del Regolamento Europeo 2016/679 come una violazione di particolare gravità in quanto associata ad **una sanzione pecuniaria fino a 20 milioni di euro ovvero fino al 4% del fatturato mondiale globale annuo**

POTERI DELL'AUTORITA'

Anche **la mancata osservanza della richiesta di fornire informazioni** è qualificata (ai sensi dell'art. 166, comma 2, del D.lgs. n.196/2003 come modificato dal D.lgs. n. 101/2018, come una violazione di particolare gravità in quanto associata ad una **sanzione pecuniaria fino a 20 milioni di euro ovvero fino al 4% del fatturato mondiale globale annuo**

POTERI DELL'AUTORITA'

Non solo vi è una sanzione pecuniaria, ma il legislatore italiano ha previsto anche **una fattispecie penale** (ai sensi dell'art. 168, comma 2, del D.Lgs n.196/2003, così come modificato dal D.Lgs. n.101/2018) ovvero **«è punito con la reclusione fino ad un anno** *chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti*»



CONSULENZE PACI PRIVACY

Artt. 157 – 160

D.Lgs n.196/2003

Poteri di Polizia Giudiziaria per le violazioni costituenti reato

Art. 157 D.Lgs n. 196/2003 – come integrato dal D.Lgs. n. 101/2018

Nell'ambito dei poteri di cui all'art. 58 del Regolamento Europeo 2016/679

Il Garante può richiedere

↓

Al responsabile, al titolare, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di

↓ ↓

Fornire informazioni

Esibire documenti anche con riferimento alle banche dati

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Art. 158 D.Lgs n.196/2003 – come integrato dal D.Lgs n. 101/2018

Il Garante può disporre accessi

alle banche di dati

o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento

o nei quali occorre effettuare rilevazioni utili al controllo

avvalendosi, ove necessario, della collaborazione di altri organi dello Stato

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Art. 158 D.Lgs n. 196/2003 – come integrato dal D.Lgs n. 101/2018

Se gli accertamenti si svolgono in

un'abitazione

un altro luogo di privata dimora

nelle relative appartenenze

previa autorizzazione del presidente del tribunale competente per territorio

o

con l'assenso scritto ed informato del titolare o del responsabile

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Art. 159 D.Lgs n. 196/2003 – come integrato dal D.Lgs n. 101/2018

Il Garante nel procedere a rilievi e operazioni può

Estrarre copia di ogni atto, dato e documento

Anche a campione e su supporto informatico o per via telematica

Può avvalersi, ove necessario, di consulenti tecnici tenuti al segreto ai sensi dell'art. 156, comma 6

Redige al termine di ogni giornata un verbale nel quale sono descritte le operazioni svolte, raccolte le dichiarazioni rese la documentazione acquisita

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Art. 159 D.Lgs n. 196/2003 – come integrato dal D.Lgs n. 101/2018

Ai soggetti presso i quali sono eseguiti gli accertamenti viene consegnata copia dell'autorizzazione del Tribunale, ove rilasciata

Tali soggetti sono tenuti a prestare collaborazione

In caso di rifiuto gli accertamenti sono comunque eseguiti

Le spese occorrenti sono a carico del titolare con il provvedimento che definisce il procedimento

Il provvedimento costituisce titolo esecutivo ai sensi degli artt. 474 e 475 c.p.c.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

POTERI DELL'AUTORITA'

I verificatori/ispettori **non sono autorizzati a prelevare gli originali** dei documenti di interesse, bensì possono procedere all'estrazione della copia del documento o file elettronico inerente all'oggetto dell'ispezione, preservandone il contenuto.

Il personale **ispettivo riveste la qualifica di *ufficiale* o di agente di polizia giudiziaria:**

ciò comporta che, qualora nel corso dell'ispezione **emergano violazioni** penalmente rilevanti (artt. 167 – 171 del Codice), il personale addetto **possa procedere utilizzando i poteri investigativi del c.p.p.** (eseguendo per esempio perquisizioni o sequestri, anche di iniziativa).

Primo Protocollo di intesa siglato nel 2005 – Aggiornato 2016 - 2021

PROTOCOLLO D'INTESA RELATIVO AI RAPPORTI DI COLLABORAZIONE TRA IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI E LA GUARDIA DI FINANZA

… con obiettivo di regolare le reciproche forme di intesa finalizzate a porre in essere una sempre più intensa ed efficace attività di controllo sulla raccolta di informazioni.

In particolare, la Guardia di Finanza collaborerà alle attività ispettive attraverso:
•la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;

•lo sviluppo di attività delegate o sub-delegate per l'accertamento delle violazioni di natura penale ed amministrativa;

•l'assistenza nei rapporti con l'Autorità Giudiziaria;

•il reperimento di dati e informazioni sui soggetti da controllare.

•Inoltre, il Corpo collabora nell'esecuzione di indagini conoscitive sullo stato di attuazione della legge in determinati settori.

Primo Protocollo di intesa siglato nel 2005 e rinnovato nel 2016

Articolo 3 (Richieste di collaborazione)

Il Garante, in relazione alle questioni su cui ritenga necessario avvalersi della collaborazione, invia specifiche richieste al ***Nucleo Speciale Tutela Privacy e Frodi Tecnologiche***, di seguito denominato "Nucleo", il quale assicura, con proiezione nazionale, gli adempimenti connessi all'attività collaborativa avvalendosi anche dei reparti del Corpo dislocati sul territorio, i quali riferiscono al Garante per tramite del Nucleo.

1. Le richieste indicano l'ambito e lo scopo dell'intervento, i soggetti interessati, i fatti, le circostanze e le modalità in ordine ai quali è chiesto di reperire i dati e le informazioni, di fornire assistenza, di partecipare all'esecuzione delle attività ispettive e/o di sviluppare le attività delegate o sub-delegate per l'accertamento delle violazioni di natura penale o amministrativa ed ogni altra utile informazione.
2. Le richieste potranno anche riguardare pluralità di soggetti nei cui confronti svolgere accertamenti con riferimento a specifici adempimenti.
3. In relazione alle richieste, sono fornite al Nucleo documenti, informazioni ed elementi necessari per eseguire le attività di collaborazione.
4. Per il tramite del Nucleo Speciale Privacy, il Garante può richiedere la collaborazione del Nucleo Speciale Frodi Tecnologiche per tutte quelle attività di accertamento che richiedano un’elevata specializzazione in ambito telematico.

ATTIVITA' DEL NUCLEO PRIVACY

Protocollo di intesa con la Guardia di Finanza

- Il reperimento di dati ed informazioni sui soggetti da controllare
- L'assistenza nei rapporti con l'Autorità Giudiziaria
- La partecipazione di proprio personale agli accessi alle banche dati, ispezioni e verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento
- Lo sviluppo di attività delegate per l'accertamento delle violazioni di natura penale

Provvedimento del 29 dicembre 2023 - Attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo gennaio-luglio 2024 [9981356]

1. Limitatamente al periodo gennaio - luglio 2024, l'attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, è indirizzata:

a) accertamenti in ordine ai trattamenti di dati personali svolti presso gli istituti scolastici attraverso le "piattaforme di registro elettronico e suite digitali";
b) prosecuzione, tramite accessi ispettivi in loco, delle attività istruttorie concernenti gli accessi abusivi alle banche dati pubbliche (con specifico riguardo all'anagrafe tributaria ed alla banca dati INPS);
c) accertamenti nei confronti di titolari del trattamento che trattano dati personali dei dipendenti, anche ai fini valutativi, tramite sistemi informativi e dispositivi telematici installati su veicoli aziendali o presso centri logistici;
d) prosecuzione delle ispezioni sui gestori dell'identità digitale (SPID) e sulla filiera dei soggetti di cui essi si avvalgono per il rilascio di servizi fiduciari (SPID e firma digitale);
e) prosecuzione delle verifiche in ordine alla corretta implementazione delle Linee guida in materia di cookie e altri strumenti di tracciamento del 10 giugno 2021, anche attraverso lo strumento degli accertamenti on line;

Provvedimento del 29 dicembre 2023 - Attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo gennaio-luglio 2024 [9981356]

1. Limitatamente al periodo gennaio - luglio 2024, l'attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, è indirizzata:

f) accertamenti nei confronti dei titolari del trattamento che operano nel settore energetico con particolare riguardo dell'attivazione di contratti non richiesti e all'attività di valutazione dell'affidabilità della clientela;
g) accertamenti nei confronti di società che gestiscono sistemi di allarme con possibilità di connessione audio/video da remoto;
h) prosecuzione degli accertamenti in ordine ai trattamenti svolti per finalità statistiche e di ricerca scientifica sia presso uffici di statistica appartenenti al SISTAN, sia presso IRCCS;
i) programmazione, come previsto dal Regolamento (CE) 767/2008, del nuovo ciclo di attività di supervisione sui trattamenti di dati personali nel VIS (Sistema informativo dei visti);
j) accertamenti nei confronti di titolari del trattamento in ordine ai problemi concernenti il consenso al marketing e alla profilazione nonché in relazione allo svolgimento di campagne di telemarketing;
k) 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 da a) fino a k) almeno 50 accertamenti ispettivi, effettuati anche a mezzo della Guardia di finanza.

Come nasce un'ispezione e come gestirla

1) Gli accertamenti ispettivi possono scaturire a seguito di ***segnalazioni o reclami dei soggetti interessati oppure su iniziativa del Garante***, per conoscere lo stato di attuazione della normativa in determinati settori pubblici e privati;

2) Le attività ispettive sono condotte anche in autonomia dal ***Nucleo Speciale Tutela Privacy e Frodi Tecnologiche*** della Guardia di Finanza. Nei casi più gravi e in cui sono richieste competenze specifiche maggiori, funzionari del Garante procedono personalmente alle ispezioni con o senza il supporto della GdF ed accompagnati da consulenti/tecnici;

3) Le ispezioni possono avvenire con preavviso (di solito via pec) dal Garante o dalla GdF tramite una comunicazione (spesso solo il giorno prima) ma possono anche avvenire a sorpresa.
Si consiglia di formare chi controlla la PEC affinchè valuti l'importanza di tale comunicazione e avverta subito i vertici, il Privacy Team, il Rpd in modo da prepararsi all'arrivo degli ispettori/verificatori;

4) Al momento dell'accesso in sede, previa evidenza del tesserino di riconoscimento, l'ispettore/verificatore presenta il documento ove è indicata la richiesta di informazioni;

5) È opportuno dotarsi di una procedura interna affinché siano avvisati i vertici dell'organizzazione e, ove possibile, siano presenti. In ogni caso dovrà essere presente un referente del Privacy Team, il Rpd, ed eventuali fornitori esterni (in particolare Ads);

6) Fondamentale la verbalizzazione delle attività svolte e delle dichiarazioni di cui si desidera lasciare traccia. Si suggerisce di verificare sempre la correttezza di quanto dichiarato, anche al fine di limitare i rischi di sanzioni penali;

7) Ove possibile far verificare da un legale interno le dichiarazioni che saranno verbalizzate in modo da non riportare informazioni che si possano rivelare controproducenti o contraddittorie;

8) Laddove, nell'interlocuzione con l'ispettore/verificatore non si sia sicuri di quanto dichiarato, è bene attendere e riservarsi di rispondere successivamente. Gli ispettori/verificatori potrebbero avere necessità di prelevare copia dei documenti rilevanti ai fini della verifica (informative, contratti, policy, istruzioni ecc.);

10) In genere vengono assegnati 15 giorni (dalla notificazione della richiesta di informazioni e quindi dal primo giorno di ispezione) per l'invio di copia della documentazione richiesta. Riservarsi di inviare successivamente la documentazione piuttosto che fornirla incompleta o non aggiornata;

11) E' preferibile che per l'intero arco temporale dell'ispezione, ci sia sempre il medesimo referente in modo da coordinare i lavori e fare da punto di riferimento per gli ispettori/verificatori;

12) Le ispezioni possono durare anche diversi giorni. A fine giornata è consigliabile che venga svolto un report interno delle attività svolte, allegando anche copia del verbale rilasciato e, ove possibile, l'oggetto dell'incontro del giorno successivo;

13) Prendere nota di tutti i documenti (inclusi anche banche dati, archivi, software) visionati dagli ispettori/verificatori e delle informazioni richieste e fornite;

14) Dimostrarsi collaborativi e non reticenti;

15) Rilasciare sempre informazioni veritiere e corrette (nel dubbio, non rispondere è meglio che fornire informazioni false);

16) In caso di richiesta di documentazione riservata, è consigliabile verificare di anonimizzare o cancellare le parti che non si desidera mettere a disposizione dell'Autorità (per esempio copie di buste paga, certificati, ecc);

17) Il GDPR impone la nuova prospettiva della responsabilizzazione che comporta una rendicontazione delle attività svolte al fine dimostrare la conformità dei propri trattamenti ai nuovi principi normativi. Per questa ragione è necessario tenere traccia di tutto il lavoro svolto (audit interni, attività formativa, aggiornamento documentazione ecc);

18) Se la verifica avviene con preavviso verificare che tutta la documentazione sia stata adeguatamente aggiornata.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

PRINCIPALI ADEMPIMENTI

- ❑ **Registro dei trattamenti** (Art. 30 Reg. Europeo 2016/679)
- ❑ **Informativa** (Artt. 13 e 14 Reg. Europeo 2016/679)
- ❑ **Esercizio dei diritti** (Artt. da 15 a 22 Reg. Europeo 2016/679)
- ❑ **Privacy by design e privacy by default** (Art. 25 Reg. Europeo 2016/679)
- ❑ **Ruoli nel trattamenti** (artt. da 26 a 29 Reg. Europeo 2016/679)
  (Contitolari del trattamento – Rappresentanti di titolari o di responsabili – Responsabile del trattamento)
- ❑ **Valutazione del rischio, sicurezza** (Art. 32 Reg. Europeo 2016/679)
- ❑ **Attività formativa** (Art. 29 Reg. Europeo 2016/679 e Art. 2 – quater decies D.Lgs n. 196/03
- ❑ **Procedura data breach** (Artt. 33 e 34 Reg. Europeo 2016/679)
- ❑ **Valutazione d'impatto** (Art. 35 Reg. Europeo 2016/679)
- ❑ **Nomina DPO** (Art. 37 Reg. Europeo 2016/679)

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Quali domande potrebbero essere poste dagli ispettori/verificatori

-Sono stati effettuati audit interni o presso responsabili esterni?

- Sono previste sanzioni disciplinari per i dipendenti in caso di inosservanza delle norme sul trattamento dei dati?

-Viene svolta l'attività formativa?

-Il sito Internet prevede adeguate policy?

-Quali regole sono state adottate in caso di utilizzo di impianti di videosorveglianza?

-Quali adempimenti sono stati adottati per il lavoro agile e le misure di contenimento covid-19?

Documenti richiesti

- ►*Struttura e organizzazione societaria*
- ►*Distribuzione delle funzioni privacy (Organigramma)*
- ►*Modalità con cui vengono rese le informazioni (Art. 13 e 14 GDPR), con evidenza della copia*
- ► *Modalità di acquisizione dei consensi per i contatti commerciali finalizzati trattamenti dati per la profilazione, per la cessione – comunicazione a terzi e relativa comunicazione*
- ► *Copia del Registro delle attività del trattamento (Art. 30 , se predisposto GDPR)*
- ► *Copia designazione dei Responsabili del trattamento (Art. 28 GDPR) – Fornitori di servizi*
- ► *Copia contratto designazione Responsabile della protezione dati (Artt, 37 – 38 – 39 GDPR) con rendicontazione della non designazione*
- ► *Documentazione relativa alle autorizzazioni interne, alle istruzioni ed alla formazione erogata*
- ► *Tipologie di profilazione eseguite con dettaglio del funzionamento (raccolta , aggregazione ed analisi della clientela)*
- ►*Raccolta di eventuali dati particolari per la profilazione*
- ► *Tipologie di attività di marketing effettuate a seguito della profilazione*
- ► *Periodo di conservazione dei dati di profilazione e criteri utilizzati*

Documenti richiesti

►*DPIA (Valutazione d'impatto art. 35 GDPR) eseguite per il trattamento dati di profilazione, videosorveglianza, copie e documenti*

►*Presupposti, ambito di modalità di comunicazione dei dati a terzi anche con riferimento a società controllanti, controllate o collegate*

►*Procedure per l'esercizio dei diritti agli interessati*

► *Misure tecniche ed organizzative adottate*

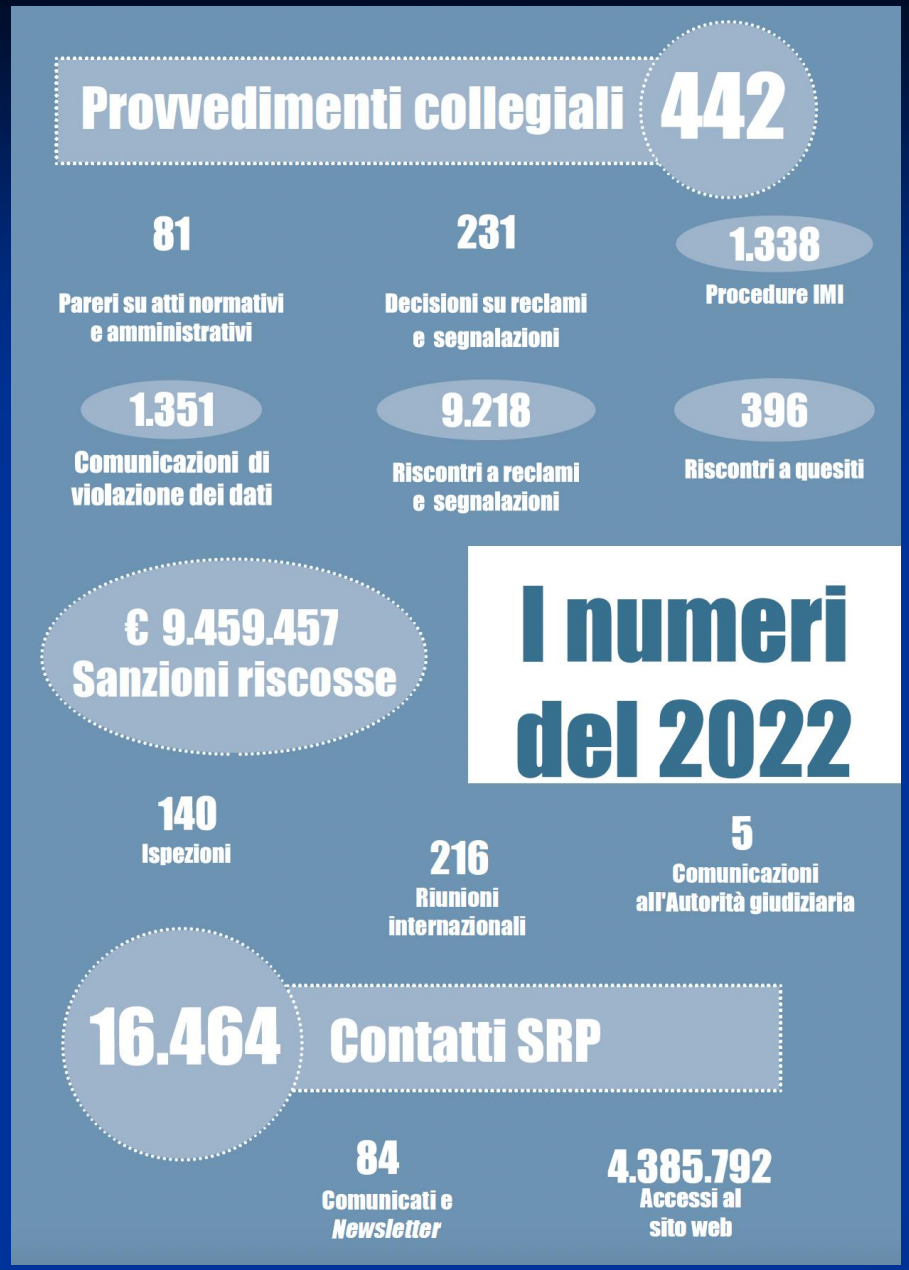
- *Eventuali tecniche di pseudonimizzazione, cifratura, procedura back up e ripristino ecc.*
- *Applicativi e servizi utilizzati sui sistemi in cloud*
- *Misure e procedure d'accesso ed autenticazione*
- *Audit effettuati ai fornitori*
- *Eventuali audit sui sistemi*

Eventuale documentazione da presentare utile ai fini dell'istruttoria

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

Numeri e statistiche
Attività dell'Autorità Garante
Relazione annuale 2022



IV - I dati statistici 2022

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	442
Pareri su norme di rango primario statale, delle regioni e delle autonomie	12
Pareri su atti regolamentari e amministrativi	69
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	24
Pareri ai sensi dell'art. 110 del Codice per la realizzazione di un progetto di ricerca medica, biomedica ed epidemiologica nonché ex art. 36 del RGPD	4
Autorizzazione di accordi amministrativi ai sensi degli artt. 46, par. 3, lett. *b*); 58, par. 3, lett. *i*) e 63 del RGPD	1
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio	94
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio con contestuale ordinanza-ingiunzione	137
Provvedimenti collegiali a seguito di notifica di violazione di dati	6
Provvedimenti collegiali a seguito di notifica di violazione di dati con contestuale ordinanza-ingiunzione	12
Provvedimenti di approvazione di codici di condotta	1
Comunicazione di violazione dei dati	1.351
Riscontri a segnalazioni e reclami (art. 11, reg. Garante n. 1/2019)	9.218
Riscontri a quesiti (art. 11, reg. Garante n. 1/2019)	396
Risposte ad atti di sindacato ispettivo e di controllo	1
Audizioni del Presidente del Garante o memorie scritte trasmesse al Parlamento	9
Contatti Servizio relazioni con il pubblico	16.464
Accertamenti e controlli effettuati *in loco* (artt. 157-158, d.lgs. n. 196/2003)	140
Pagamenti derivanti dall'attività sanzionatoria	9.459.457
Comunicazioni di notizia di reato all'Autorità giudiziaria	5
Opposizioni (trattate) a provvedimenti del Garante	123
Ricorsi giurisdizionali trattati ex art. 152, d.lgs. n. 196/2003	70
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 1, d.lgs. n. 33/2013	1
Istanze di accesso civico presentate al Garante e riscontrate ai sensi dell'art. 5, comma 2, d.lgs. n. 33/2013	14
Istanze di riesame a seguito di diniego all'accesso civico presentate al Rpct e riscontrate ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	1
Misure correttive e sanzionatorie (art. 58, par. 2, del RGDP)	317
Misure correttive e sanzionatorie (d.lgs. n. 51/2018)	2
Riunioni del Comitato europeo per la protezione dei dati personali	15
Partecipazione a sottogruppi di lavoro del Comitato europeo per la protezione dei dati personali	162
Riunioni e ispezioni autorità comuni di controllo/organismi di supervisione (Europol, SIS II, Dogane, Eurodac, VIS)	10
Conferenze internazionali	4
Riunioni presso l'OCSE e il CoE	12
Altre conferenze e incontri internazionali	13

Tabella 1. Sintesi delle principali attività dell'Autorità

Tabella 2. Attività di comunicazione dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	71
Newsletter	13
Prodotti editoriali	6
Campagne informative	10
Video *spot* e *teaser* informativi	32
Infonografiche e pagine tematiche	64

Tabella 3. Pareri ex art. 36, par. 4, del RGPD su norme di rango primario statale, delle regioni e delle autonomie

Pareri ex art. 36, par. 4, del RGPD su norme di rango primario statale, delle regioni e delle autonomie	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	3
Giustizia	1
Lavoro	3
Sanità	4
Trasporti	1
Totale	**12**

Tabella 4. Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi al Governo

Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi al Governo	
Temi	**Riscontri resi nell'anno***
Ambiente	2
Digitalizzazione p.a.	19
Diritti fondamentali	2
Fisco	6
Giustizia	2
Istruzione	4
Marketing	1
Sanità	6
Sanità: Covid-19	3
Settore privato	2
Trasporti	4
Totale	**51**

Tabella 5. Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi ad altre Istituzioni

Pareri ex art. 36, par. 4, del RGPD su atti regolamentari e amministrativi resi ad altre Istituzioni	
Temi	**Riscontri resi nell'anno***
Digitalizzazione p.a.	8
Fisco	5
Sanità	1
Statistica	4
Totale	**18**

Tabella 6. Misure correttive e sanzionatorie (art. 58, par. 2, del RGPD)

Misure correttive e sanzionatorie	
Avvertimenti a titolare/responsabile del trattamento (art. 58, par. 2, lett. *a*), del RGPD)	7
Ammonimenti a titolare/responsabile del trattamento (art. 58, par. 2, lett. *b*), del RGPD)	44
Ingiunzioni a titolare/responsabile del trattamento a soddisfare le richieste dell'interessato concernenti l'esercizio dei diritti riconosciuti dal RGPD (art. 58, par. 2, lett. *c*), del RGPD)	28
Ingiunzioni a titolare/responsabile del trattamento di conformare i trattamenti alle disposioni del RGPD (art. 58, par. 2, lett. *d*), del RGPD)	35
Ingiunzioni a titolare del trattamento di comunicare all'interessato una violazione dei dati personali (art. 58, par. 2, lett. *e*), del RGPD)	3
Imposizioni di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento (art. 58, par. 2, lett. *f*), del RGPD)	25
Ordine di rettifica/cancellazione di dati personali o limitazione del trattamento ex artt. 16, 17 e 18 e altre misure previste dall'art. 58, par. 2, lett. *g*), del RGPD)	23
Sanzioni amministrative pecuniaria ex art. 83 (art. 58, par. 2, lett. *i*), del RGPD)	149
Ordine di sospensione dei flussi di dati verso un destinatario in un Paese terzo o un'organizzazione internazionale, ai sensi dell'art. 58, par. 2, lett. *j*), del RGPD	3
Totale	**317**

Tabella 7. Misure correttive e sanzionatorie (d.lgs. n. 51/2018)

Misure correttive e sanzionatorie	
Sanzioni amministrative pecuniarie (art. 42, d.lgs. n. 51/2018)	2
Totale	**2**

Tabella 8. Comunicazioni di notizia di reato all'Autorità giudiziaria

Comunicazioni di notizia di reato all'Autorità giudiziaria	
Violazioni in materia di controlli a distanza dei lavoratori (art. 171, d.lgs. n. 196/2003)	3
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168, d.lgs. n. 196/2003)	2
Totale	**5**

Tabella 9. Pagamenti derivanti dall'attività sanzionatoria

Pagamenti derivanti dall'attività sanzionatoria	
Pagamenti spontanei dei contravventori	7.273.875,91
Riscossione coattiva	2.185.581,15
Totale	**9.459.457,06**

Tabella 10. Cooperazione tra autorità nazionali di protezione dei dati personali in IMI (Capo VII RGPD)*

Cooperazione tra autorità nazionali di protezione dei dati personali - procedure IMI (Capo VII RGPD)		
1) Decisioni finali adottate nell'ambito della attività di cooperazione rispetto alle quali il Garante ha agito in qualità di:		**222**
a)"autorità capofila" (LSA)	8	
b)"autorità interessata" (CSA)	214	
2) Procedure preliminari ex art. 56 del RGPD		**601**
a) Procedure preliminari pervenute rispetto alle quali l'Autorità si è dichiarata "autorità interessata"	370	
b) Procedure preliminari pervenute rispetto alle quali l'Autorità si è dichiarata "autorità non interessata"	180	
c) Procedure preliminari pervenute rispetto alle quali l'Autorità ha assunto il ruolo di "autorità capofila"	7	
d) Procedure preliminari pervenute rispetto alle quali l'Autorità ha fornito altro riscontro	4	
e) Procedure preliminari promosse dall'Autorità	4	
f) Altro	36	
3) Procedure di cooperazione ad impatto esclusivamente locale ex art. 56, par. 2, del RGPD		**0**
4) Procedure di cooperazione informale ex art. 60 del RGPD rispetto alle quali vi è stata una partecipazione dell'Autorità in qualità di:		**65**
a)"autorità interessata"	62	
b)"autorità capofila"	3	
5) Progetti di decisione ex art. 60 del RGPD rispetto ai quali l'Autorità ha cooperato in qualità di:		**235**
a1)"autorità interessata"	212	
a2)"autorità interessata" e rispetto ai quali sono state sollevate "obiezioni pertinenti e motivate" o commenti ex art. 60, par. 4, del RGPD	21	
b)"autorità capofila"	2	
6) Richieste di assistenza reciproca ex art. 61 del RGPD		**210**
a) ricevute da altre autorità	180	
b) inviate ad altre autorità	30	

Tabella 11. Procedure IMI nell'ambito del meccanismo di coerenza

Meccanismo di coerenza - procedure IMI (Capo VII RGDP)	
Procedure relative all'attività decisoria dell'EDPB per la risoluzione delle controversie ex art. 65 del RGPD con la partecipazione dell'Autorità	4
Procedure d'urgenza ex art. 66 del RGPD	1

Tabella 12. Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza

Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza	
Assicurazioni	8
Associazioni	2
Biometria	1
Concessionari	1
Credito	57
Dati in ambito pubblico	11
Dati in ambito sanitario	10
Diritto all'oblio	32
Imprese	181
Informazioni commerciali	1
Lavoro	8
Liberi professionisti	2
Libertà di espressione e di informazione	15
Notificazioni di violazione dei dati	79
Recupero crediti	7
RGPD	3
Reti telematiche	915
Sistema sanzionatorio	1
Trasferimento dati all'estero	1
Videosorveglianza	2
Altro	1
Totale	**1338**

Tabella 13. Segnalazioni e reclami

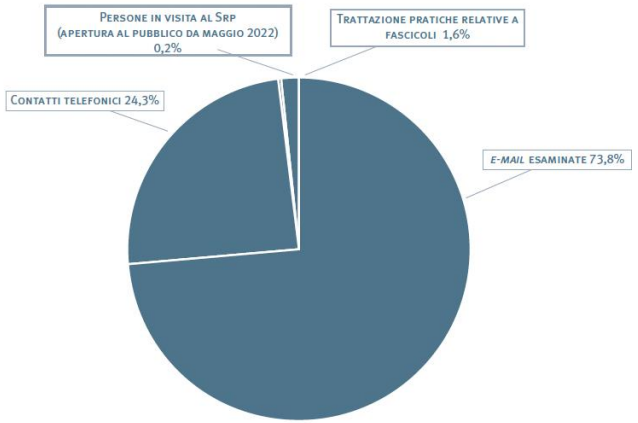
Segnalazioni e reclami	Pervenuti nell'anno	Riscontri resi nell'anno (*)
Attività ispettive	0	28
Affari legali e giustizia	163	119
Intelligenza artificiale	1	0
Libertà di manifestazione del pensiero e cyberbullismo	774	888
Realtà economiche e produttive	2.867	2.990
Realtà pubbliche	1.569	881
Reti telematiche e *marketing*	24.867	3.687
Sanità e ricerca	579	559
Tecnologie digitali e sicurezza informatica	60	66
Totale	**30.880**	**9.218**

Tabella 14. Quesiti

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
Attività ispettive	1	2
Affari legali e giustizia	18	14
Libertà di manifestazione del pensiero e cyberbullismo	6	7
Realtà economiche e produttive	148	203
Realtà pubbliche	187	101
Reti telematiche e *marketing*	45	23
Sanità e ricerca	49	46
Tecnologie digitali e sicurezza informatica	3	0
Totale	**457**	**396**

Tabella 15. Servizio relazioni con il pubblico

Servizio relazioni con il pubblico	
E-mail esaminate	12.154
Contatti telefonici	4.000
Persone in visita al Srp (apertura al pubblico da maggio 2022)	40
Trattazione pratiche relative a fascicoli	270
Totale	**16.464**



(*) inerenti anche ad affari pervenuti anteriormente al 2022

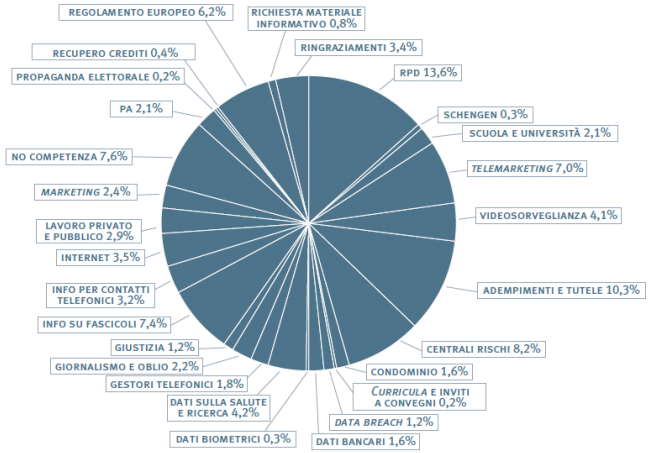


Grafico 16. Oggetto delle *e-mail* esaminate dal Servizio relazioni con il pubblico

Personale in servizio (*)				
Area	ruolo (a)	fuori ruolo (b)	comandato presso altre amm.ni o in aspettativa (c)	impiegato dall'Ufficio (a+b-c)
Segretario generale	0	1	0	1
Dirigenti	17	0	1	16
Funzionari	91	4	2	93
Operativi	25	0	0	25
Esecutivi	2	0	0	2
Totale	**135**	**5**	**3**	**137**
Personale a contratto (art. 156, comma 5, del Codice)				11

Tabella 17. Personale in servizio

Risorse finanziarie				
Entrate accertate	**Anno 2022**	**Anno 2021**	**Variazione**	
Entrate correnti	44.584.987	35.627.273	8.957.714	25,14%
Altre entrate, trasferimenti e rimborsi	726.554	342.242	384.312	112,29%
Totale entrate	**45.311.541**	**35.969.515**	**9.342.026**	**25,97%**
Spese impegnate	**Anno 2022**	**Anno 2020**	**Variazione**	
Spese di funzionamento	33.347.228	25.280.392	8.066.836	31,91%
Spese in c/capitale	448.728	624.459	-175.731	-28,14%
Trasferimenti ad amministrazioni	380.968	333.451	47.517	14,25%
Totale spese	**34.176.924**	**26.238.302**	**7.938.622**	**30,26%**

Valori in euro

Tabella 18. Risorse finanziarie

(*) Situazione alla data del 31/12/2022

ACCOUNTABILITY

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

Prevenire è meglio che curare

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il valore degli audit per il rispetto di policy, procedure, attività formative, protocolli quali parti integranti del metodo organizzativo privacy

Perché con il Regolamento Europeo 2016/679 gli audit devono essere diversi da quelli svolti in precedenza?

1) Cambiato il perimetro di tutela (dalla tutela del dato alla tutela dei diritti e libertà delle persone fisiche);
2) Molti adempimenti che prima erano impliciti ora devono essere formalizzati pena l'applicazione di sanzioni, laddove non adottati;
3) Sono stati introdotti nuovi principi e concetti, primo fra tutti *l'accountability* ma anche *privacy by design e by default* che hanno impatti significativi sulle attività di audit

Quali documenti preparare in relazione ai principali adempimenti

- ☐ Procedure standard in relazione a determinati trattamenti (es. riscontro richieste di esercizio dei diritti);
- ☐ Relazioni relative a determinati trattamenti (es.videosorveglianza - biometria);
- ☐ *Policy* interne in materia di protezione dei dati (regolamento per il recepimento del GDPR, o un altro atto ufficiale, organigramma / funzionigramma eventualmente grafico, in grado di descrivere i ruoli interni rispetto al trattamento dei dati per ciascun dipartimento/settore/servizio ecc);
- ☐ Procedure adottate per l'attività formativa;
- ☐ Procedure adottate per l'esercizio dei diritti;
- ☐ Istruzioni o procedure per la pubblicazione degli atti nell'area trasparenza per effetto del D.Lgs. 33/2013;
- ☐ Istruzioni o procedure per la gestione delle richieste di accesso 241/90
- ☐ Istruzioni o procedure per la gestione dell'albo pretorio
- ☐ Documenti attestanti l'adozione di *best practice (buone prassi)* o eventuali certificazioni in materia di sicurezza o protezione dei dati (evidenza dell'avvenuta valutazione in merito all'adozione delle misure dell'AGID)
- ☐ Policy per la conservazione dei dati cartacei (presenza di dotazione di distruggi documenti in numero e postazioni adeguate, gestione delle chiavi di uffici e armadi dotati di serratura, verifica delle stampe in uscita presso le stampanti ubicate in spazi comuni non presidiati)
- ☐ Documentazione di procedimenti avanti il Garante

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

Parere 3/2010 sul principio di responsabilità

Adottato il 13 luglio 2010

53. «Esistono vari metodi a disposizione dei responsabili del trattamento per valutare l'efficacia (o l'inefficacia) delle misure. Per il trattamento di dati di maggiori dimensioni, più complesso e ad alto rischio, gli audit interni ed esterni sono metodi comuni di verifica. Anche il modo in cui vengono condotti gli audit può variare, da audit completi ad audit negativi (che possono a loro volta assumere forme diverse)».

Nel decidere come garantire l'efficacia delle misure, il Gruppo di lavoro articolo 29 suggerisce di utilizzare gli stessi criteri applicati per decidere le misure mutuati dall'articolo 17 della direttiva 95/46/CE, vale a dire, ***i rischi*** *presentati dal trattamento e la natura dei dati*. Pertanto, il modo in cui un Titolare del trattamento deve assicurare l'efficacia delle misure dipende dalla sensibilità dei dati, dalla quantità dei dati trattati e dai particolari rischi che il trattamento comporta.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

Parere 3/2010 sul principio di responsabilità

Adottato il 13 luglio 2010

- Attività di audit quale strumento a disposizione del titolare per valutare e quindi dimostrare la conformità alla norma;
- La mancanza di evidenze costituisce una violazione della norma sanzionabile, facilitando l'attività dell'auditor;

- Attività di audit non è solo uno strumento per verificare la conformità alla norma, ma anche per verificare cosa si è fatto, cosa si sta facendo o si potrebbe fare per ridurre i rischi di non conformità (*violazione dati personali – principio privacy by design e by default*)

Le diverse tipologie di audit

- Audit in ambiti formalizzati con precetti dettati dalla norma (informative – designazioni – basi giuridiche);
- Audit in ambiti non formalizzati la norma lascia al Titolare la facoltà di decidere (misure di sicurezza – analisi dei rischi)
- Audit in temi specifici (Ads – videosorveglianza – biometria)
- Audit tecnici/organizzativi (tempi di conservazione dei dati, esercizio dei diritti, qualità dei dati)

Laddove non sia disponibile un elenco specifico con gli adempimenti da eseguire è importante far riferimento a documenti e buone prassi derivanti dall'Autorità di controllo dei singoli Paesi – Enisa (Agenzia Europea per la cibersicurezza - ISO (29134, 29151…).

Così come accade per le altre tipologia di compliance che sia per la tutela della sicurezza nei luoghi di lavoro, per l'ambiente, per la qualità, nel sistema di gestione di data protection, un audit deve avere sempre fissato un obiettivo chiaro e condiviso, che può essere per esempio:

- verificare il grado di conformità alla normativa vigente;
- verificare il grado di conformità alle policy di data protection, ovvero i regolamenti di data protection interni dettati dal Titolare del trattamento, che tutti i dipendenti sono tenuti ad osservare.
- accertare il livello di conformità al GDPR e alle data protection policy aziendali di un fornitore di servizi che implichino la gestione e/o il trattamento di dati, (es. un call center in outsourcing, o semplicemente il consulente del lavoro che elabora le buste paga), al fine di valutare che i requisiti dichiarati e concordati nella fase iniziale di stesura dell'accordo, sia stati rispettati e mantenuti nel tempo;
- accertare l'efficacia di azioni correttive intraprese a seguito di "non conformità" scaturite da un precedente audit di verifica.

La corretta gestione di un'attività di audit prevede la formalizzazione di un ***piano di audit*** all"interno del quale vengono esplicitati preventivamente:

-Gli obiettivi che si intendono raggiungere con l'attività di audit;
-I criteri che verranno adottati per raggiungere gli obiettivi di cui sopra, e quali sono i documenti di riferimento utilizzati; (ad. esempio policy, regolamenti interni, procedure operative ecc.)
-Il campo operativo dell'audit quindi quali unità organizzative saranno coinvolte dalla verifica;
-I giorni e i luoghi in cui verrà effettuato l'audit;
- Il tempo stimato che è necessario per effettuare le verifiche in presenza, (ciò consente di allocare correttamente le risorse interne che dovranno essere coinvolte nell'attività di verifica);
-La lingua da utilizzare nel corso delle attività di audit, nel caso di contesti internazionali;
-La check list di domande (preferibilmente aperte) da utilizzare come supporto operativo che consentano di raggiungere il giusto livello di approfondimento.

Tale piano va condiviso prima di iniziare l'effettiva attività di audit, durante una riunione di apertura per consentire la comprensione delle attività che si andranno a svolgere da parte di tutte le risorse coinvolte.

Domande che devono essere poste in sede di audit per la verifica degli adempimenti posti in essere dal Titolare:

- Effettuato e documentato una analisi dei rischi sui diritti e le libertà delle persone fisiche?
- Definito ed implementato misure tecnico/organizzative ai fini di garantire la sicurezza ai sensi degli artt. 25 e 32?
- Definito ed implementato misure tecnico/organizzative per la gestione delle violazioni di dati personali?
- Definito ed implementato misure tecnico/organizzative per la gestione dei diritti degli interessati?

Domande che devono essere poste in sede di audit per la verifica degli adempimenti posti in essere dal Titolare:

- Individuato e formalizzazione le misure per il trasferimento di dati all'estero?
- Formalizzato l'eventuale designazione del DPO, dei relativi compiti e posizionamento?
- Formalizzata la valutazione delle competenze e caratteristiche del DPO?

Ha predisposto una procedura per la valutazione della corretta base giuridica del trattamento?

- Ha predisposto una procedura per la valutazione delle condizioni che consentono il trattamento dei dati di cui agli artt. 9 e 10?

Domande che devono essere poste in sede di audit per la verifica degli adempimenti posti in essere dal Titolare:

- Ha predisposto una procedura per la corretta formulazione della richiesta del consenso, là dove è richiesto?
- Ha predisposto una procedura per la gestione del consenso nel tempo?
- Ha predisposto una procedura per la corretta gestione della richiesta del consenso per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori?
- Ha predisposto una procedura per la verifica della condizione in cui un minore possa esprimere il consenso?

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Definite le aree di maggiore rischio, le successive verifiche devono avvenire con il livello di dettaglio che dovrà essere valutato dall'auditor

POLITICHE PER IL TRATTAMENTO DEI DATI E RESPONSABILIZZAZIONE (Art. 5 e 24 Reg. EU 2016/679)
Sono state redatte politiche per il trattamento dei dati con previsione di aggiornamento e revisione che comprovano l'applicazione dei principi del Reg. EU 2016/679?

SONO STATI INDIVIDUATI I RUOLI DI TITOLARITA', CO-TITOLARITA' RESPONSABILE, E DESIGNATI AL TRATTAMENTO DEI DATI ?

E' STATO PREDISPOSTO IL REGISTO DELLE ATTIVITA' DEL TRATTAMENTO (Art. 30 Reg. EU 2016/679) del ttitolare e del Responsabile?

INFORMATIVE E CONSENSO (Art. 13-14, 6 e 7 Reg. EU 2016/679):
Sono state predisposte le corrette informative per i soggetti interessati, individuate le basi giuridiche del trattamento e ove necessario richiesto e registrato il consenso ? es. marketing, profilazione, etc.:

FORMAZIONE (Art. 29 Reg. EU 2016/679):
La formazione è alla base della conoscenza, consapevolezza e responsabilizzazione. E' stato redatto un piano di formazione già all'ingresso in servizio di un dipendente, anche sulla base degli specifici trattamenti dati ?

VENGONO UTILIZZATI IMPIANTI PER LA RILEVAZIONE DELLE PRESENZE MEDIANTE RICONOSCIMENTO BIOMETRICO O MEDIANTE GEOLOCALIZZAZIONE ? E' stata verificata l'aderenza alle prescrizioni e provvedimenti dell'Autorità Garante, valutazione per la indispensabilità / accountability

POLICY SITO WEB:
Sono pubblicate sul sito internet aziendale le corrette informazioni per il trattamento dei dati dei navigatori, utenti, anche in presenza di moduli di raccolta dati, newsletter, profilazione, gestione dei consensi e cookie?:

SONO STATE VERIFICATE LE GARANZIE ADEGUATE PER IL TRASFERIMENTO DI DATI PERSONALI IN PAESI EXTRA-UE?
in applicazione delle raccomandazioni del EDPB (Gruppo dei Garanti Europei)

NOMINE A RESPONSABILE (ESTERNO) ES. FORNITORI/CONSULENTI ESTERNI (Art.28 Reg. EU 2016/679):
Sono state predisposte le nomine a responsabile per ciascun soggetto esterno che tratta dati per conto del titolare o responsabile?

AMMINISTRATORI DI SISTEMA: (Provv. 27 novembre 2008 (G.U. n. 300 del 24/12/2008)
Sono state predisposte le nomine per l'amministratore di sistema *interno*, e/o *esterno* se presente?

La conduzione dell'Audit, prevede la raccolta e la verifica delle informazioni attraverso osservazioni dirette del processo, l'esame documentale, le interviste ai referenti del processo/area da auditare. Tutte le evidenze raccolte devono essere **documentate e verificabili**, basate su un campione delle informazioni disponibili poiché l'audit deve essere svolto su un periodo di tempo limitato. I risultati e l'esito complessivo dell'audit, quindi le conclusioni, devono essere documentate attraverso un audit report. Le risultanze dell'audit, che possono essere classificate in:

- non conformità,
- osservazioni/opportunità di miglioramento,
- commenti/raccomandazioni

Inoltre, il report deve contenere o richiamare le modalità per correggere/colmare le carenze rilevate. I contenuti del rapporto di audit devono essere comunicati **attraverso una riunione di chiusura** con il management dell'azienda, e condivise con le funzioni/aree/dipartimenti auditati, affinchè possano attivarsi per risolvere le non conformità rilevate con le opportune azioni correttive.

I tipi di verifica che rilevano in ambito privacy sono, principalmente:

- l'autovalutazione degli adempimenti effettuati dal Titolare/Responsabile tramite strutture interne (audit/compliance) o esterne
- la valutazione degli adempimenti effettuati dal DPO anche per il tramite di strutture interne (audit/compliance) o esterne
- la valutazione di un Titolare sugli adempimenti contrattuali del Responsabile
- la valutazione di un Titolare sugli adempimenti contrattuali del DPO (intesa semplicemente come corrispondenza fra l'operato del DPO e quanto concordato contrattualmente, senza entrare nel merito delle modalità con cui tali attività sono state svolte)
- la valutazione di un Titolare sui requisiti del DPO.

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

Grazie per l'attenzione