GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

PALAZZO DI GIUSTIZIA
FIRENZE

Il titolare del trattamento ed il DPO: sinergie operative nel corso dell'attività ispettiva

Claudio Filippi
Vice Segretario generale e
Dirigente del Dipartimento attività ispettive

INDICE DEGLI ARGOMENTI PRINCIPALI

- **Premessa**
- **I poteri di accertamento e ispettivi del Garante nel quadro dell'attività istruttoria dell'Autorità e la collaborazione con la Guardia di finanza;**
- **I soggetti coinvolti nell'attività ispettiva: il ruolo del titolare e del DPO.**

QUESTIONE DI ACCOUNTABILITY!

"Before I write my name on the board, I'll need to know how you're planning to use that data."

PREMESSA

I cittadini italiani sono tra i meno consapevoli dell'esistenza di una normativa che protegge i loro diritti fondamentali

Il 23 maggio 2019, **l'Eurobarometro**, in occasione dell'anniversario del GDPR ha chiesto ad un campione i 1.000 persone per ciascuno dei 28 Stati Membri «***se fossero a conoscenza dell'esistenza del GDPR***».

La popolazione svedese è risultata la **più informata** (90%) seguita da quella olandese (87%), polacca (86%) e ceca (85%).

L'Italia è al penultimo posto con il 49% degli intervistati che afferma di sapere cosa è il Regolamento 2016/679 o, quantomeno, di averne sentito parlare.

Nel complesso, il 67% dei cittadini UE sa che esiste il GDPR.

L'indagine rivela anche che **il 57% degli europei** è a conoscenza che nel proprio paese c'è un'Autorità preposta alla protezione dei loro diritti sui dati personali;

il 43% degli italiani non è consapevole dell'esistenza di un authority competente in materia (solo il **18% degli italiani conosce il Garante per la Protezione dei Dati Personali**).

Privacy: indagine in 18 Paesi, carenze per imprese e enti pubblici

(AGI) - Roma, 5 mar. – Si è svolta una indagine a tappeto ("sweep") in 18 Paesi (Italia inclusa) a cura delle Autorità di protezione dati appartenenti al *Global Privacy Enforcement Network (GPEN)* **per *verificare il rispetto del principio di accountability* in Europa ai sensi del nuovo Regolamento**.

Privacy: indagine in 18 Paesi e i risultati in Italia

RISULTATI ITALIANI - L'indagine ha coinvolto **19 soggetti pubblici (Regioni e Provincie autonome) e 54 società *in-house*.**

Viene giudicato

«Molto grave» la gestione della valutazione dei rischi:

il **24% delle societa' in-house e il 58% delle Regioni** non hanno processi documentati per la «valutazione dei rischi» sulla protezione dei dati personali, in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi.

***il 20%* delle Regioni non tiene traccia** neanche dei dati personali comunicati o trasmessi a terzi.

I risultati dell'indagine: in Italia

Viene giudicato

«grave» la gestione delle richieste e dei reclami:

il 48% delle Regioni e il 24% delle società non hanno policy e procedure per la gestione delle richieste e dei reclami da parte degli interessati o delle stesse Autorità;

«carente» la gestione degli incidenti di sicurezza (Data Breach):

il 20% delle organizzazioni non ha ancora implementato una procedura di risposta agli incidenti di sicurezza che includa, tra l'altro, la notifica all'Autorità e, in caso di alto rischio per le libertà e i diritti degli interessati, anche la comunicazione a questi ultimi".

Il 25% delle organizzazioni non dispone di un registro per documentare le violazioni subite.

Accountability e pubblicazione online di una circolare contente dati sensibili di alunni minorenni

La Corte dei Conti si è pronunciata su un'istanza della Procura regionale a carico della dirigente e di alcuni docenti di un istituto professionale "*per asserito danno indiretto cagionato all'ente di appartenenza derivante dall'avere pubblicato sulla rete internet una circolare contente* ***dati idonei a rivelare lo stato di salute di scolari minori affetti da disabilità****, così ledendo il diritto alla riservatezza loro e delle famiglie, e, per l'effetto, causando l'irrogazione ad opera del Garante per la Protezione dei dati personali di una sanzione amministrativa, per violazione dell'art. 22, comma 8, del Codice, di* ***€ 20.000,00*** *soddisfatta con fondi appartenenti alla scuola*".

La Corte ha stabilito che "gli obblighi normativi […] sono stati dunque disattesi dalla Dirigente scolastica, che con la sua **condotta gravemente sprezzante** degli stessi ha leso il diritto alla tutela della riservatezza del minore, causando per sua esclusiva colpa (personale ed *in vigilando*) l'irrogazione della sanzione [provvedimento del Garante n. 36127/97738 del 22.12.2015], così da **creare un danno, indiretto, alle casse dell'Istituto scolastico**, in quanto il pagamento di somme con denaro pubblico **a causa dell'inosservanza di obblighi imposti normativamente** costituisce un aggravio di spesa e sottrae le relative somme all'attuazione degli scopi istituzionali».

La Corte, in applicazione del potere riduttivo dell'addebito, ha condannato la Dirigente scolastica […] al «pagamento, in favore dell'Istituto Professionale di Stato […], della somma di **€ 7.500,00** […]», specificando altresì «l'impossibilità di ritenere responsabili della pubblicazione della circolare in parola gli altri docenti rispetto ai quali "è emerso il loro ruolo marginale, di ***meri esecutori delle istruzioni diramate dalla Dirigente scolastica*** […]"».

(Corte dei Conti - sentenza n. 246 del 28 maggio 2019)

I poteri del Garante

(artt. 51-54 Regolamento e artt. 153, 154, 154-bis, 154-ter)

INVESTIGATIVI	CORRETTIVI	AUTORIZZATIVI E CONSULTIVI	PROCEDURE LEGALI
• **Richiedere informazioni e condurre indagini** • **Effettuare controlli** • **Riesaminare le certificazioni** • **Ottenere accesso alle informazioni e ai locali**	• Impartire ordini, avvertimenti, richiami • Vietare un trattamento • Ritirare una certificazione • Infliggere sanzioni	• Consultazione preventiva e autorizzazioni • Codici di condotta e certificazioni • Clausole contrattuali standard e norme vincolanti d'impresa (*BCR*)	• Legittimato agire in giudizio in caso di violazioni disposizioni in materia di protezione dei dati personali (art. 154-ter Codice)

Gli Stati Membri possono prevedere ulteriori poteri (art. 58, § 6, Regolamento e art. 154-bis Codice)

LA POTESTA' ISPETTIVA ESERCITATA DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

I compiti di indagine nel Regolamento n. 2016/679/UE

Il Regolamento individua tra i compiti del Garante lo svolgimento di:

«***indagini sull'applicazione del regolamento***, *anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica*» (art. 57, lett. h).

Il controllo ispettivo

L'attività ispettiva è lo strumento istruttorio necessario per **accertare *in loco*** situazioni di fatto che devono essere oggetto di valutazione da parte dell'Autorità in relazione a specifici casi.

Tale attività è utilizzata anche con lo scopo di acquisire conoscenze in relazione a **fenomeni nuovi** in vista di una successiva regolazione da parte del Garante nell'ambito delle attribuzioni allo stesso rimesse dal Regolamento e dal Codice.

Il Garante effettua in media 280 ispezioni all'anno

LA PROGRAMMAZIONE ISPETTIVA

Le ispezioni sono effettuate **sulla base di programmi** elaborati secondo **linee di indirizzo** stabilite dal Garante con delibere di programmazione che indicano **gli ambiti del controllo e gli obiettivi numerici** da conseguire.

Le linee generali della programmazione dell'attività ispettiva vengono quindi rese pubbliche attraverso il sito *web* del Garante e, sulla base dei criteri così fissati, **l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo** e istruisce i conseguenti procedimenti.

La programmazione ispettiva per il **I° semestre 2019** è stata adottata con delibera del 14 febbraio 2019 *[doc. web n. 9096661].*

Individuazione della platea dei soggetti da sottoporre a controllo

LE IMPRESE IN ITALIA

Fonte: elaborazioni Ufficio Studi Confcommercio su dati Istat

I dati quantitativi

Le **imprese attive** in Italia nell'industria e nei servizi di mercato sono ***4.338.766*** di unità.

Le PMI sono 4.335.446

La composizione

- Le **microimprese** (quelle con meno di 10 addetti) sono ***4.117.489*** e rappresentano il ***95,4%***.
- Le **piccole imprese** (quelle da 10 a 49 addetti) sono 196.090 e rappresentano il **4,1%**;
- Le **medie imprese** (quelle da 50 a 249 addetti) sono 21.867 e rappresentano lo **0,5%**;
- Le **grandi imprese** (quelle con almeno 250 addetti) sono 3.320 unità e rappresentano < **0,1%.**

Le esigenze di semplificazione delle micro, piccole e medie imprese

1. Il Garante ha il potere di «*adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento*». In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, come definite dalla raccomandazione 2003/361/CE, il Garante promuove, nelle linee guida di indirizzo, «***modalità semplificate di adempimento degli obblighi del titolare del trattamento***». (Art. 154-*bis Codice).*

2. L'obbligo di tenuta di un **registro delle attività di trattamento non si applica** alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento presenti un rischio per i diritti e le libertà dell'interessato, o includa categorie particolari di dati o i dati personali relativi a condanne penali e a reati.

3. In funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese, si incoraggia l'elaborazione di **codici di condotta** destinati a contribuire alla corretta applicazione del Regolamento (art. 40 Regolamento).

4. Nell'incoraggiare l'istituzione di **meccanismi di certificazione** della protezione dei dati nonché di **sigilli e marchi** di protezione dei dati allo scopo di dimostrare la conformità al Regolamento, sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese (art. 42 Regolamento).

I poteri di indagine nel Regolamento

Ogni autorità di controllo ha i seguenti **poteri di indagine** **(art. 58 § 1)**:

- ingiungere al titolare e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare o del responsabile del trattamento, **di fornirle ogni informazione** di cui necessiti per l'esecuzione dei suoi compiti (lett. a);
- condurre **indagini** sotto forma di **attività di revisione** sulla protezione dei dati (lett. b);
- 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 (lett. e);
- 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, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri (lett. f).

Il dlgs 10 agosto 2018, n. 101

In attuazione della delega conferita al Governo dall'art. 13 della legge n. 163 del 2017, **il dlgs 10 agosto 2018, n. 101, ha adeguato l'ordinamento italiano** alle previsioni del Regolamento 2016/679/UE anche nello **specifico settore dei controlli.**

Le modifiche apportate al Codice dal dlgs. N. 101/2018
LA RICHIESTA DI INFORMAZIONI

NOVITA'

Il Garante, per l'espletamento dei propri compiti, **può richiedere** al titolare, al responsabile (**e ora anche ai suoi rappresentanti**), all'interessato o anche a terzi **di fornire informazioni e di esibire documenti *anche con riferimento al contenuto di banche di dati*** (art. 157).

GLI ACCERTAMENTI

Il Garante **può disporre:**

- **accessi a banche di dati, archivi** o
- **altre ispezioni e verifiche nei luoghi** ove si svolge il trattamento o nei quali occorre **effettuare rilevazioni** comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali (art. 158 Codice).

I «particolari accertamenti»

I ***particolari accertamenti*** riguardano i trattamenti effettuati per motivi di **sicurezza e difesa dello Stato**.

Tali controlli sono effettuati per il tramite di **un componente** designato dal Garante e i documenti acquisiti sono custoditi assicurandone la **segretezza** e sono conoscibili dal presidente e dai componenti del Garante e, se necessario, da un numero delimitato di addetti all'Ufficio individuati dal Garante.

Per gli accertamenti relativi agli **organismi di informazione e di sicurezza** e ai dati coperti da **segreto di Stato** il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante (art. 160)

Il **Regolamento n. 1/2019**. Procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, nonché all'adozione dei provvedimenti correttivi e sanzionatori. (Delibera n. 98) (**GU n.106 del 8-5-2019**).

Attività ispettive e di revisione sulla protezione dei dati personali (Art. 22)

1. Il dipartimento attività ispettive cura lo svolgimento dell'attività ispettiva (**artt. 157 e 158 Codice e art. 58, § 1, e art. 62 RGPD**) tenuto anche conto della **programmazione** dell'attività ispettiva disposta dal Collegio sulla base di un **ordine di servizio** sottoscritto dal dirigente del medesimo dipartimento.

2. L'attività ispettiva può essere curata dal dipartimento ovvero **delegata alla Guardia di finanza**. La stessa può essere altresì effettuata avvalendosi, ove necessario, della collaborazione di altri organi dello Stato.

3. Valutata la sussistenza di eventi di particolare rilevanza, **il Collegio può disporre ulteriori attività ispettive.**
4. Il dipartimento attività ispettive **cura altresì i controlli** nell'ambito delle istruttorie preliminari e dei procedimenti amministrativi comunque **avviati presso altre unità organizzative** dell'Autorità, alle quali è restituito l'esito per la successiva trattazione.

Segue: il **Regolamento n. 1/2019**

Attivita' ispettive e di revisione sulla protezione dei dati personali (Art. 22)

L'ordine di servizio con cui è disposta l'attività ispettiva individua:

1. il titolare o il responsabile del trattamento destinatari del controllo;
2. i poteri di indagine utilizzati, l'ambito del controllo, il luogo ove si svolge l'accertamento;
3. il responsabile delle attività e gli ulteriori partecipanti;
4. le sanzioni previste ai sensi dell'art. 83, paragrafo 5, lettera e), del RGPD e degli articoli 166 e 168 del Codice.

Nel corso dell'attività ispettiva, della quale può essere dato preavviso, **è possibile, in particolare**:

a. controllare, estrarre ed acquisire copia dei documenti, anche in formato elettronico;
b. richiedere informazioni e spiegazioni;
c. accedere alle banche dati ed agli archivi;
d. acquisire copia delle banche dati e degli archivi su supporto informatico.

Una peculiare forma di controllo: l'attività di revisione

NOVITA'

Le attività di revisione sulla protezione dei dati personali sono avviate ai sensi dell'art. 58, paragrafo 1, lettera b), del RGPD, **presso il titolare o il responsabile del trattamento ovvero presso la sede dell'Autorità**. In tale ultimo caso, l'attività si svolge a seguito di convocazione del titolare o del responsabile presso il dipartimento attività ispettive e di revisione.

Nell'ambito delle attività di revisione, qualora emergano elementi di criticità nel trattamento dei dati personali, **possono essere avviate attività ispettive** al fine di rilevare eventuali violazioni della normativa sulla protezione dei dati personali.

In relazione all'attività svolta, alle dichiarazioni rese e ai documenti acquisiti, è **redatto processo verbale**, una copia del quale viene consegnata al soggetto sottoposto ad ispezione ovvero ad attività di revisione.

COSA SUCCEDE SE ……

- **In caso di mancato riscontro alla richiesta di informazioni** ai sensi dell'art. 157 del Codice (art. 83, §5 del Regolamento (art. 15 c. 1, dlgs. n. 101/2018; art. 166 Codice);
- **ovvero di negato accesso ai dati e ai locali (art. 83, §5, lett. e) del Regolamento):**

Si configura una violazione amministrativa per la quale è previsto il pagamento di una somma fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato

---

- Qualora in un procedimento o nel corso di accertamenti dinanzi al Garante, **chiunque dichiari o attesti falsamente notizie o circostanze o produce atti o documenti falsi, si configura un illecito penale punito con la reclusione da sei mesi a tre anni**

- Qualora **chiunque intenzionalmente cagioni un'interruzione o turbi** la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti (art. 168 Codice) **si configura un illecito penale punito con la reclusione sino ad un anno.**

LE MODALITA' DI CONTROLLO
Le garanzie

Anche il Regolamento dispone che ogni Paese disponga di:

«Garanzie appropriate per l'esercizio del potere dell'Autorità nello svolgimento delle attività ispettive e di controllo» *(v. art. 58, c. 4).*

Il nuovo Codice aggiornato dal dlgs. 10 agosto 2018 n. 101
Le garanzie «appropriate»

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.

Costituisce poi una **novità** la possibilità che, sulla base delle predette garanzie, il Garante possa **effettuare accertamenti** in luoghi privati per il **controllo su reti di comunicazione accessibili al pubblico**, e **acquisire dati e informazioni** *on line.*

Il nuovo Codice aggiornato dal dlgs. 10 agosto 2018 n. 101
LA COLLABORAZIONE CON LA GdF

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

Protocollo di intesa del 10 marzo 2016

Il Protocollo d'intesa del 10 marzo 2016

La Guardia di Finanza - Nucleo Speciale Tutela Privacy e Frodi Tecnologiche collabora con il Garante alle attività ispettive attraverso:

- il **reperimento di dati e informazioni** sui soggetti da controllare;
- la **partecipazione agli accessi** alle banche dati, **ispezioni, verifiche** e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
- l'assistenza nei **rapporti con l'Autorità Giudiziaria**;
- lo sviluppo di **attività delegate o sub-delegate** per l'accertamento delle violazioni in materia di protezione dei dati personali;
- la partecipazione di proprio personale, a richiesta del Garante, a **ispezioni congiunte con autorità di protezione dei dati personali appartenenti ad altri Paesi**.

Il Protocollo d'intesa del 10 marzo 2016

La Guardia di Finanza collabora altresì:

- nell'esecuzione di indagini conoscitive sullo stato di attuazione della legge in **determinati settori**;
- nell'esecuzione, a richiesta del Garante, di **verifiche *on-line***, volte a rilevare, dall'esame dei siti *web* e degli altri strumenti telematici utilizzati, il rispetto della disciplina di protezione dei dati personali da parte dei **titolari, pubblici e privati**, che effettuano trattamenti di dati personali per mezzo di reti telematiche;
- alla progettazione e attuazione, d'intesa con il Garante, di altre iniziative, anche nell'ambito della cooperazione internazionale.

La Guardia di Finanza provvede inoltre a segnalare al Garante tutte le situazioni rilevanti di cui venga a conoscenza nel corso dell'esecuzione delle ordinarie attività di servizio.

IL COORDINAMENTO E LA COOPERAZIONE TRA DPA EUROPEE

L´autorità di controllo capofila e la cooperazione prevista dal meccanismo di "sportello unico"

Il Regolamento istituisce le **"autorità di controllo"** in ciascuno Stato membro con **identici compiti e poteri** (artt. 57 e 58) in tutti i Paesi Ue **introducendo la nozione di "autorità di controllo capofila"** per i trattamenti transfrontalieri (art. 56) .

Le «operazioni congiunte» delle autorità di controllo «la funzione ispettiva»

Il Regolamento amplia notevolmente gli **spazi di collaborazione tra le autorità di controllo** prevedendo che esse debbano fornire **assistenza reciproca anche per condurre operazioni congiunte**, in particolare per lo svolgimento di indagini o per il controllo dell'attuazione di misure nei confronti di un titolare del trattamento o responsabile del trattamento stabilito **in un altro Stato membro**.

A tale scopo ciascuna autorità mette in atto misure per cooperare efficacemente con le altre condividendo le informazioni acquisite e **prevedendo di effettuare ispezioni e indagini in collaborazione**, attivandosi anche al fine di favorire la trasmissione di informazioni utili sullo svolgimento di un'indagine.

Le c.d. «indagini congiunte»

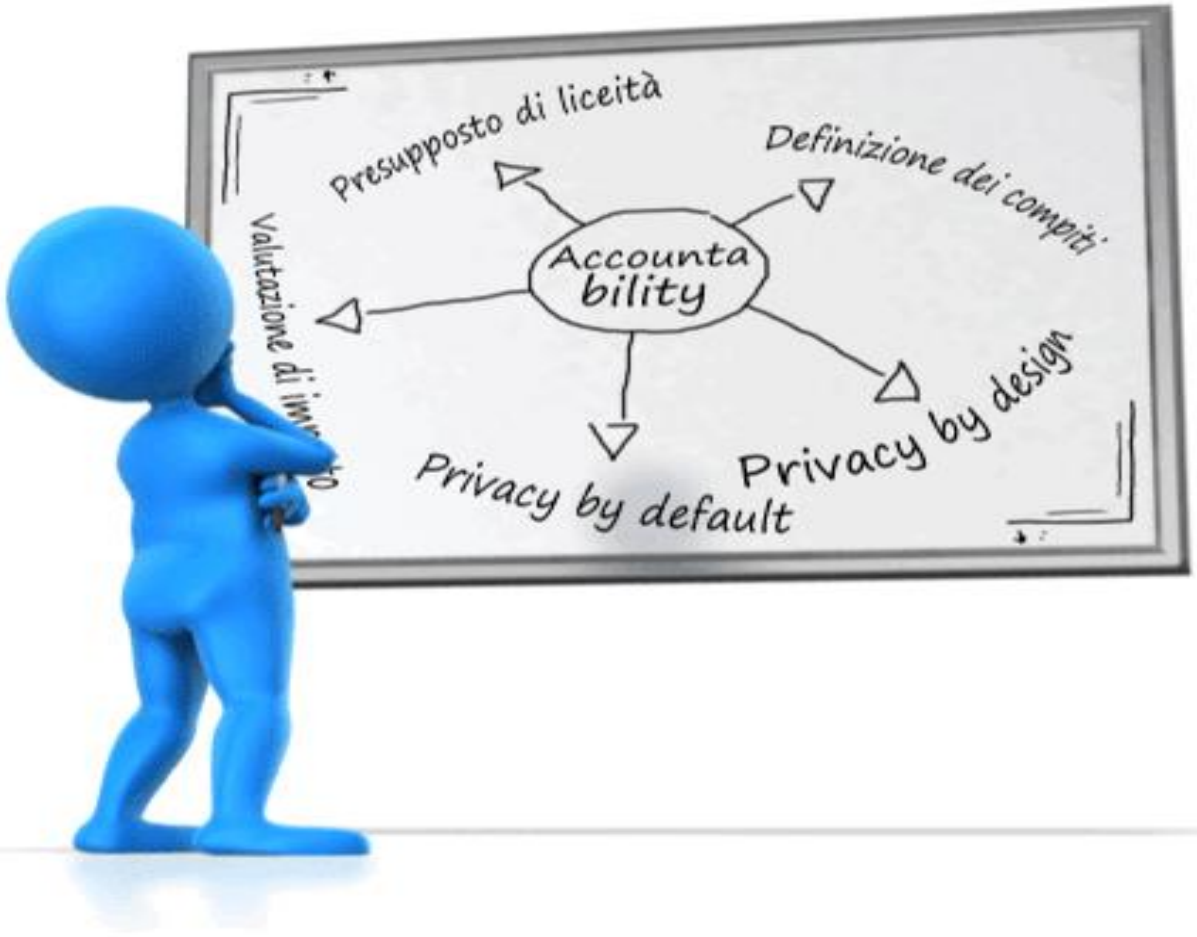
Nei casi in cui siano condotte **operazioni congiunte**, è possibile che si svolgano **anche indagini congiunte** cui partecipano membri o personale di autorità di controllo di altri Stati membri.

L'autorità di controllo competente invita l'autorità di controllo di ogni Stato membro interessato a partecipare all'operazione congiunta.

Novità l'autorità di controllo può, in conformità al proprio diritto interno e con l'autorizzazione dell'autorità di controllo ospitata, **conferire poteri, anche d'indagine, ai membri o al personale dell'autorità di controllo ospitata che partecipano alle operazioni congiunte** o **consentire di esercitare i loro poteri d'indagine** in conformità al diritto dello Stato membro dell'autorità di controllo ospitata. Tali poteri d'indagine possono essere esercitati **unicamente sotto il controllo e in presenza di membri o personale dell'autorità di controllo.**

La responsabilizzazione e l'interazione con l'Autorità: un sistema ancora in costruzione

Necessità di un approccio sistemico



I soggetti coinvolti nell'attività ispettiva: il ruolo del titolare e del DPO

Accountability e approccio basato sul rischio

Il principio di *accountability* ambisce a realizzare il passaggio da una concezione di adempimento formale ad un approccio sostanziale di protezione dei dati, connesso alla natura delle attività concretamente svolte, all'analisi dei rischi e alle misure di sicurezza che risultino adeguate alle singole fattispecie.

Accountability e approccio basato sul rischio

Il GDPR adotta taluni "strumenti" al fine di rafforzare la tutela dei dati e la responsabilizzazione del Titolare e del Responsabile del trattamento:

- sancisce i principi della *privacy by design* (in progettazione pseudonimizzazione/minimizzazione) e della *privacy by default* (impostazione predefinita solo dati necessari per singola finalità) (art. 25);
- prevede la tenuta del Registro dei trattamenti (art. 30);
- richiede di implementare adeguate misure di sicurezza, tenendo in considerazione le tipologie di operazioni svolte e i relativi livelli di rischio, affinché non si verifichino violazioni dei dati (art. 32 ss);
- prevede la valutazione d'impatto (art. 35);
- introduce la figura del Data Protection Officer (art. 37).

Soggetti: compiti del titolare

GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79

Il titolare:

- Individua il rischio connesso al trattamento;
- Pone in sicurezza l'attività di trattamento dei dati;
- Mette in atto misure tecniche e organizzative adeguate a garantire che il trattamento è effettuato conformemente al Regolamento;
- Rilascia l'informativa all'interessato;
- Attende all'esercizio dei diritti dell'interessato;
- **Fornisce dimostrazione** che il trattamento è effettuato conformemente al Regolamento;
- Designa il/i Responsabile/i del trattamento dei dati (outsourcing);
- Vigila sull'osservanza del contratto con cui sono designati tali Responsabili;

Soggetti: compiti del titolare (e contitolarità)

GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79

- Compila il registro del trattamento dei dati;
- Nomina il Responsabile della Protezione dei dati (DPO/RPD);
- Coopera con l'Autorità di controllo;
- Notifica l'eventuale violazione dei dati personali (*data breach*);
- Documenta la violazione dei dati personali (*data breach*);
- Comunica la violazione dei dati personali (*data breach*);
- Effettua la «valutazione d'impatto» (DPIA);
- Effettua la «consultazione preventiva».

Contitolarità:
È possibile che coesistano più titolari del trattamento che decidono congiuntamente di trattare i dati per una finalità comune. In tale caso, i contitolari devono definire specificamente, con un **atto giuridicamente valido**, il rispettivo ambito di responsabilità e i compiti. Gli interessati, però, possono rivolgersi indifferentemente ad uno qualsiasi dei contitolari.

IL RESPONSABILE del trattamento dei dati

ESCLUSIVAMENTE CON UN CONTRATTO (o altro atto giuridico) E' DISCIPLINATA:

- Materia, durata, natura e finalità del trattamento;
- tipo di dati personali e categorie di interessati;
- **obblighi e diritti** del titolare del trattamento.

IN BASE AL CONTRATTO IL RESPONSABILE SI IMPEGNA A:

- trattare dati soltanto **su istruzione documentata del titolare**;
- consentire i trattamenti **solo a persone autorizzate** con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le **misure di sicurezza** (es. cifratura; pseudonimizzazione; recupero da backup);
- rispettare le **condizioni per ricorrere a un sub-responsabile** del trattamento;
- assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- **cancellare o restituire** tutti i dati e cancellare le copie esistenti;
- mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.

Soggetti: **autorizzati** al trattamento

Non c'è una esplicita definizione della figura delle persone autorizzate al trattamento.

Si ricava dall'art. 4.10 del Regolamento UE 2016/679, dove vengono definite come **non "terzo"** le persone autorizzate al trattamento dei dati personali che operano sotto l'autorità diretta del titolare o del responsabile e dall'art. 29 del Regolamento UE 2016/679.

L'art. 29 stabilisce che le persone autorizzate al trattamento dei dati personali non possono trattare tali dati se non sono **istruite** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli stati membri.

Soggetti: il responsabile della protezione dei dati (RPD)

Il **responsabile della protezione dei dati (RPD)** è al centro di questo nuovo quadro giuridico in molti ambiti ed è chiamato a facilitare l'osservanza delle disposizioni del RGPD.

Vi è l'obbligo di nominare un RPD:

- se il trattamento è svolto da un'**autorità pubblica** o da un organismo pubblico (ivi compresi soggetti che svolgono funzioni pubbliche o esercitano pubblici poteri);
- se **le attività principali** del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala (es. impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali); oppure
- se **le attività principali** del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

APPROFONDIMENTO: le attività principali

Esempio

Tutti gli organismi (pubblici e privati) svolgono le attività di pagamento delle retribuzioni al personale o di predisposizione di strutture standard di supporto informatico.

Si tratta di **funzioni di supporto** necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo **necessarie o essenziali** sono considerate solitamente **accessorie** e **non vengono annoverate fra le attività principali**.

Soggetti: la responsabilità dei responsabili della protezione dei dati (RPD)

Il **responsabile della protezione dei dati** ha, fra gli altri, il compito di sorvegliare l'osservanza del RGPD.

Nel considerando 97 si specifica che il titolare o il responsabile del trattamento dovrebbe essere "*assistito [dal RPD] nel controllo del rispetto a livello interno del presente regolamento*".

Fanno parte di questi compiti di controllo svolti dal RPD, in particolare:

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità,
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile. (artt. 37-39).

Il controllo del rispetto del regolamento **non significa che il RPD sia personalmente responsabile in caso di inosservanza**. Il RGPD chiarisce che spetta al titolare, e non al RPD, "*mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*" (art. 24, paragrafo 1).

Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del RPD.

Soggetti: i responsabili della protezione dei dati (RPD)

ALCUNI ESEMPI

- Un gruppo imprenditoriale può nominare **un unico responsabile della protezione dei dati**, a condizione che tale responsabile sia facilmente raggiungibile da ciascuno stabilimento.
- **Qualora il titolare o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.**

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

Il responsabile della protezione dei dati può essere un dipendente del titolare o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Il titolare o il responsabile del trattamento **pubblica i dati di contatto del responsabile** della protezione dei dati e li comunica all'Autorità di controllo.

Accountability e approccio basato sul rischio: DPO

GDPR: art. 38 e considerando 97

IL GARANTE ACCERTA NELL'ISPEZIONE CHE

Il titolare e il responsabile del trattamento:

si assicurino che il DPO sia tempestivamente e adeguatamente **coinvolto** in tutte le questioni riguardanti la protezione dei dati personali.

si assicurino che il DPO **non riceva alcuna istruzione** per quanto riguarda l'esecuzione di tali compiti. Il DPO **non è rimosso o penalizzato dal titolare o dal responsabile del trattamento per l'adempimento dei propri compiti**. Il DPO **riferisce direttamente al vertice gerarchico** del titolare o del responsabile del trattamento.

sostengano il DPO nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le **risorse necessarie** per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Accountability e approccio basato sul rischio: DPO

GDPR: art. 38 e considerando 97

IL GARANTE ACCERTA NELL'ISPEZIONE CHE

- **Gli interessati possano contattare il DPO** per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

- **Il DPO** pur potendo svolgere altri compiti e funzioni, sia assicurato (a cura del titolare o del responsabile del trattamento) che tali compiti e funzioni non diano adito a un **conflitto di interessi.**

Accountability e approccio basato sul rischio: DPO

GDPR: art. 39 e considerando 97

IL GARANTE ACCERTA NELL'ISPEZIONE CHE

Il DPO sia incaricato almeno dei **COMPITI** di:

a) **informare e fornire consulenza al titolare o al responsabile** del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) **sorvegliare l'osservanza del regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi **l'attribuzione delle responsabilità , la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo**;

c) **fornire, se richiesto, un parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento (art. 35);

d) **cooperare con il Garante**;

e) **fungere da punto di contatto per il Garante** per questioni connesse al trattamento, tra cui la consultazione preventiva (v. art. 36), ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

METTIAMOCI AL LAVORO…..
UNA TIPICA VALUTAZIONE DEL TITOLARE

Il concetto di «larga scala»

Il concetto di «**larga scala**» a cui fa riferimento il GDPR è rinvenibile:

- ai fini dell'**obbligo di nomina del D.P.O. (art. 37);**
- Nello svolgimento della **valutazione di impatto (art. 35)**.

Configura, inoltre, illecito penale:

- la **comunicazione e diffusione illecita** di dati personali oggetto di trattamento su «**larga scala**» e
- l'**acquisizione con mezzi fraudolenti** di un archivio automatizzato contenente dati personali oggetto di trattamento su «**larga scala**» (art. 167-bis e art. 167-ter dlgs. n. 101/2018).

Il legislatore comunitario fa solo un generico riferimento a trattamenti di notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati (cfr. Considerando 91)

Che cosa si intende, dunque, per trattamento su «**larga scala**» in tali casi? Come si devono regolare, in concreto, imprenditori, professionisti ed enti pubblici?

I fattori che qualificano la «larga scala»

Linee-guida del WP29 sui responsabili della protezione dei dati - 5 aprile 2017

Al fine di capire se il trattamento di dati è svolto su larga scala **si deve tener conto dei seguenti fattori**:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Esempi di «larga scala»

Alcuni esempi di trattamento su larga scala sono:

- trattamento di dati relativi a **pazienti** svolto da un **ospedale** nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro **tracciamento** attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile del trattamento specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento di dati relativi alla clientela da parte di una **compagnia assicurativa o di una banca** nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un **motore di ricerca** per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di **fornitori di servizi telefonici** o telematici.

Non devono, invece, ritenersi su larga scala, ad esempio:

- i trattamenti di dati relativi a **pazienti** svolti da singoli professionisti sanitari;
- i trattamenti di dati personali relativi a condanne penali e reati svolti da **singoli avvocati.**

Elementi da accertare in caso di violazioni per l'applicazione delle sanzioni amministrative pecuniarie

1. la **natura, la gravità e la durata della violazione tenendo in considerazione** la **natura, l'oggetto o la finalità del trattamento** in questione nonché il **numero di interessati lesi dal danno** e il **livello del danno da essi subito**;
2. il carattere **doloso** o **colposo** della violazione;
3. le **misure adottate** dal titolare del trattamento o dal responsabile del trattamento **per attenuare il danno subito** dagli interessati;
4. il **grado di responsabilità** del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 (by design/by default) e 32 (misure sicurezza);
5. ***eventuali*** **precedenti violazioni** pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
6. il **grado di cooperazione con l'autorità di controllo** al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
7. le **categorie di dati** personali interessate dalla violazione;
8. la **maniera in cui l'autorità di controllo ha preso conoscenza della violazione**, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione (data breach);
9. **qualora siano stati precedentemente disposti provvedimenti** di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo **stesso oggetto**, il **rispetto di tali provvedimenti**;
10. l'**adesione ai codici di condotta** approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
11. eventuali altri **fattori aggravanti o attenuanti** applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

GRAZIE PER L'ATTENZIONE

Garante per la protezione dei dati personali
Piazza Venezia 11 - 00186 ROMA
Sito www.gpdp.it – www.garanteprivacy.it
Centralino telefonico: (+39) 06.696771
E-mail: garante@gpdp.it – urp@gpdp.it
Pec: protocollo@pec.gpdp.it