



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

**Data**  
SME



GIURISPRUDENZA  
DIPARTIMENTO  
DI ECCELLENZA  
2018-2022

# IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI: TRA DISCIPLINA EUROPEA E ADEGUAMENTO DELLA DISCIPLINA NAZIONALE

# Focus fonti normative



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Inquadramento costituzionale
- La privacy in Europa
- Il “Pacchetto protezione dati”
- La riforma del Codice Privacy

Si ripercorre l’attività giurisprudenziale della Corte costituzionale italiana che ha portato al riconoscimento del diritto alla privacy all’interno dell’ordinamento italiano.

Successivamente, viene descritta l’affermazione del diritto alla privacy nel quadro giuridico europeo, con particolare riferimento alla CEDU, alla Carta dei diritti fondamentali dell’Unione europea, ai Trattati istitutivi dell’Unione e al Pacchetto protezione dati che ha portato all’adozione del GDPR.

Sono illustrati, infine, gli interventi normativi condotti in Italia in materia di privacy e di protezione dei dati personali: la legge 675/1996, sostituita dal Decreto legislativo n. 196/2003, da ultimo modificato dal Decreto legislativo n. 101/2018 per garantire l’adeguamento al GDPR.

# Oggetto e finalità



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Oggetto e finalità
- L'ambito di applicazione materiale
- L'ambito di applicazione territoriale

Lo scopo del GDPR è di garantire la protezione dei dati riguardanti le persone fisiche e, allo stesso tempo, di favorire la circolazione dei dati all'interno dell'Unione europea.

È analizzato l'ambito di applicazione materiale del Regolamento, assieme all'indicazione dei casi in cui il GDPR non trova applicazione.

Inoltre, è esaminato l'ambito di applicazione territoriale in base al quale il GDPR si applica sia ai soggetti che trattano dati personali essendo stabiliti all'interno dell'Unione, sia a coloro che, nonostante siano stabiliti in Paesi extra europei, svolgono attività di trattamento su interessati che si trovano nell'Unione.

# Definizioni



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Interessato, titolare del trattamento, responsabile del trattamento
- Categorie particolari di dati

Sono passate in rassegna le definizioni dei soggetti coinvolti nelle attività di trattamento dei dati personali. In particolare, la nozione di interessato (il soggetto a cui si riferiscono i dati trattati), nonché di titolare e di responsabile del trattamento (i soggetti che trattano i dati personali).

È analizzata inoltre la definizione di categorie particolari di dati personali. In primo luogo, viene messo in evidenza il divieto generale di trattare tali categorie di dati personali contenuto nel GDPR. In secondo luogo, vengono indagate le eccezioni previste dall'articolo 9, paragrafo 2, del GDPR ed attraverso le quali è possibile trattare dati appartenenti a categorie particolari.

# Principi



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## Aspetti principali:

- Liceità, correttezza e trasparenza
- Finalità
- Minimizzazione
- Esattezza
- Conservazione
- Integrità e riservatezza
- Responsabilizzazione

Sono analizzati i principi generali enunciati all'articolo 5 del GDPR e sulla base dei quali deve essere ispirata qualsiasi attività di trattamento di dati personali.

A tale scopo, sono richiamati i pareri e le linee guida dell'Article 29 Working Party e del Comitato europeo per la protezione dei dati.

# Liceità del trattamento – Basi giuridiche



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Consenso
- Esecuzione di un contratto e di misure pre-contrattuali
- Adempimento di un obbligo legale
- Interesse vitale dell'interessato o di un terzo
- Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri
- Legittimo interesse del titolare del trattamento

Vengono analizzate le basi giuridiche individuate all'articolo 6 del GDPR perché un trattamento di dati personali possa essere considerato lecito.

Con particolare riferimento al consenso, sono indicati gli elementi essenziali che devono essere rispettati affinché si possa ritenere che il predetto consenso sia stato rilasciato liberamente.

Inoltre, per quanto riguarda l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, sono esaminate le disposizioni della normativa italiana (es. art. 2-ter del Codice della Privacy) e le disposizioni del GDPR appositamente dedicate.



# Soggetti



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## Aspetti principali:

- Titolare del trattamento
- Contitolari del trattamento
- Responsabile del trattamento
- Soggetti che agiscono sotto l'autorità del responsabile o del titolare del trattamento

Vengono descritti i ruoli, i poteri e gli obblighi dei soggetti coinvolti nel trattamento dei dati personali.

In particolare, sono analizzate le modalità di ripartizione dei compiti e delle responsabilità tra i contitolari del trattamento. Allo stesso modo, vengono esaminati gli obblighi che il responsabile del trattamento è tenuto a rispettare e che devono essere puntualmente indicati all'interno della sua nomina.

Infine, viene descritto il processo interpretativo in base al quale è possibile individuare all'articolo 29 del GDPR un'ulteriore figura, oltre al titolare e al responsabile del trattamento, ossia il soggetto che tratta i dati sotto la loro autorità dei soggetti sopra menzionati.

# Informativa



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## Aspetti principali:

- Contenuto dell'informativa
- Tempi dell'informativa
- Modalità dell'informativa

Sono esaminati i contenuti essenziali che devono essere indicati all'interno dell'informativa, secondo quanto previsto dagli articoli 13 e 14 del GDPR.

È messo in evidenza l'obbligo generale di sottoporre l'informativa all'interessato prima dell'inizio di qualsiasi trattamento dei dati personali.

Inoltre, si osserva come le informative debbano essere predisposte affinché risultino trasparenti e facilmente comprensibili da parte dell'interessato.



# Diritti degli interessati



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## Aspetti principali:

- Diritto di accesso
- Diritto di rettifica
- Diritto alla cancellazione (Diritto all'oblio)
- Diritto alla limitazione
- Diritti alla portabilità
- Diritto di opposizione
- Diritto di non essere sottoposto a decisioni automatizzate

Viene analizzato ciascun diritto che il GDPR riconosce all'interessato: sia i diritti già previsti all'interno della Direttiva 95/46/CE sia i nuovi introdotti dal Regolamento (ad esempio il diritto all'oblio e il diritto alla portabilità).

Sono inoltre esaminate le ipotesi in cui il GDPR introduce talune restrizioni all'esercizio dei diritti degli interessati.

# Accountability e approccio basato sul rischio



Data



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Privacy by design e Privacy by default
- Registro dei trattamenti
- Codici di condotta e certificazioni
- Misure di sicurezza
- Violazione dei dati personali (data breach)
- Valutazione d'impatto
- Consultazione preventiva
- Responsabile per la protezione dei dati personali (DPO)

Sono analizzati i principi di privacy by design e by default. Tali principi impongono grande attenzione alla protezione dei dati sin dal momento della progettazione delle attività di trattamento e richiedono che, di default, vengano processati soltanto i dati necessari al perseguimento delle finalità sottese al trattamento.

# Accountability e approccio basato sul rischio



Data



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Vengono descritti i casi in cui il titolare del trattamento è obbligato a tenere un registro dei trattamenti, nonché i relativi contenuti. Al riguardo, sono richiamate le FAQ fornite dall'Autorità di controllo italiana con riguardo al registro dei trattamenti.

I codici di condotta e le certificazioni sono esaminati quali strumenti utili al titolare del trattamento per dimostrare la propria conformità al GDPR. Sono illustrati, inoltre, gli obblighi di comunicazione che il titolare del trattamento, a seconda dei casi, deve assolvere nei confronti dell'Autorità di controllo e/o degli interessati in caso di violazione dei dati personali.

Vengono analizzati la valutazione d'impatto (DPIA), da effettuare prima dell'inizio di qualsiasi trattamento qualora vi sia un rischio elevato per i diritti e le libertà delle persone fisiche, e la consultazione preventiva, da rivolgere all'Autorità di controllo nel caso in cui la DPIA riveli un elevato livello di rischio che non può essere ridotto. Per quanto riguarda la DPIA, è richiamato il parere dell'Art. 29 Working Party che fornisce 9 criteri attraverso cui valutare se si renda necessario lo svolgimento di una DPIA su un determinato trattamento.

È descritta la figura del responsabile della protezione dei dati con i relativi compiti: assistenza al titolare del trattamento; monitoraggio del rispetto del GDPR; punto di contatto tra il titolare del trattamento e l'interessato/Autorità di controllo.

# Trasferimento di dati verso Paesi terzi



## Aspetti principali:

- Principio generale per il trasferimento
- Trasferimento sulla base di una decisione di adeguatezza
- Trasferimento soggetto a garanzie adeguate
- Deroghe

Vengono analizzati i principi generali per il trasferimento di dati personali verso Paesi al di fuori dell'Unione europea, ai quali viene richiesto di garantire un livello adeguato di protezione dei dati.

In primo luogo, è esaminato lo strumento delle decisioni di adeguatezza attraverso cui la Commissione europea riconosce l'esistenza di garanzie adeguate in un Paese terzo. Vengono poi analizzate le ulteriori garanzie che possono essere adottate per il trasferimento di dati nelle ipotesi in cui non sia stata adottata una decisione di adeguatezza. Infine, sono indicate le modalità eccezionali previste dall'articolo 49 del GDPR in base alle quali, in particolari situazioni, possono essere effettuati trasferimenti verso Paesi terzi.

# Autorità di controllo



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## Aspetti principali:

- Caratteristiche, compiti e poteri
- Autorità di controllo italiana: il Garante per la protezione dei dati personali
- Autorità capofila e meccanismo dello sportello unico (one stop shop)
- Meccanismo di coerenza
- Comitato europeo per la protezione dei dati

Sono descritte le competenze, i poteri e gli obblighi che il GDPR assegna a ciascuna Autorità di controllo.

Vengono analizzati il meccanismo di coerenza e il meccanismo dello sportello unico introdotti dal GDPR per garantire un'applicazione omogenea della nuova disciplina e per assicurare un'uniforme attività delle Autorità di controllo all'interno dell'Unione europea.

Infine, vengono esaminati la composizione e il ruolo del Comitato europeo per la protezione dei dati che ha sostituito l'Art. 29 Working Party.

# Forme di tutela



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Forme di tutela
- Rappresentanza degli interessati
- Diritto al risarcimento e responsabilità

Sono descritte le tre distinte forme di tutele attraverso cui l'interessato può rivolgersi all'Autorità di controllo o all'Autorità giudiziaria: il diritto di presentare un reclamo all'Autorità di controllo, il diritto a un ricorso giurisdizionale effettivo contro la decisione di un'Autorità di controllo e il diritto a un ricorso giurisdizionale effettivo contro nei confronti del titolare del trattamento.

In questo senso, sono inoltre esaminate le disposizioni del Codice della Privacy riguardanti le forme di tutela riconosciute all'interessato.

Si osserva infine la possibilità che l'interessato sia rappresentato da un ente, un'organizzazione o un'associazione senza scopo di lucro regolarmente costituita, come previsto dall'articolo 80 del GDPR.

# Sanzioni



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Condizioni generali per infliggere sanzioni
- Sanzioni amministrative e pecuniarie
- Sanzioni penali

Sono descritti i principi che devono essere presi in considerazione nel calcolo delle sanzioni da imporre qualora siano state violate talune disposizioni del GDPR.

Vengono analizzate le due categorie di sanzioni amministrative di cui all'articolo 83 del GDPR: da un lato, le sanzioni fino a 10.000.000.000€ o fino al 2% del fatturato totale mondiale annuo dell'esercizio precedente; dall'altro lato, le sanzioni fino a 20.000.000.000€ o fino al 4% del fatturato totale mondiale annuo dell'esercizio precedente.

Si osserva inoltre la possibilità riconosciuta dall'articolo 84 del GDPR a ciascuno Stato membro di introdurre ulteriori tipologie di sanzione all'interno del proprio ordinamento, ivi comprese le sanzioni penali.

A tal riguardo, sono esaminate le sanzioni penali introdotte in Italia dal Codice della Privacy.



# Privacy e diritto del lavoro



Data



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Normativa lavoristica italiana
- Strumenti utilizzati per svolgere la prestazione lavorativa
- Email e Internet
- Videosorveglianza
- Geolocalizzazione

È analizzato il rapporto tra il diritto alla privacy e il diritto al lavoro.

Viene esaminata la normativa lavoristica italiana, con particolare riguardo all'articolo 4 della legge 300/1970 avente ad oggetto l'utilizzo di strumenti volti a rendere la prestazione lavorativa e di strumenti di controllo sul lavoratore.

La relazione tra privacy e diritto del lavoro viene approfondita attraverso l'analisi di specifici aspetti (ad esempio l'uso dell'email e di Internet, la videosorveglianza, l'utilizzo di badge, la geolocalizzazione), di pronunce della Corte Europea dei Diritti dell'Uomo, di opinioni dell'Article 29 Working Party, di provvedimenti del Garante per la protezione dei dati personali e di circolari dell'Ispettorato nazionale del lavoro.

# Marketing e profilazione



Data



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Aspetti principali:

- Legittimo interesse e marketing
- Soft spam
- Telemarketing
- Processo decisionale automatizzato relativo alle persone fisiche

È analizzato il ruolo che l'interesse legittimo può svolgere come base giuridica per i trattamenti con finalità di marketing.

Sono esaminate questioni specifiche come la soft spam e il telemarketing. A questo proposito, sono richiamati diversi provvedimenti dell'Autorità di controllo italiana.

Inoltre, viene esaminata la profilazione nell'ambito dei processi decisionali automatizzati, attraverso l'analisi dell'articolo 22 del GDPR e delle linee guida che l'Art. 29 Working Party ha elaborato sul tema.