GDPR: nuovi diritti e strumenti per la tutela dei dati personali

INDICE – GDPR: nuovi diritti e strumenti per la tutela dei dati personali

Parte 1 – *Parte 2*

I poteri del Garante Privacy nel GDPR

Privacy, trasparenza e GDPR: implicazioni e linee guida per il rapporto tra privacy e accesso ai documenti

Vantaggi strategici del GDPR: investimento essenziale per aziende e PA

Linee guida per il trattamento etico dei dati personali relativi alle informazioni commerciali

Misure di sicurezza e responsabilità per i fornitori aderenti

Codice di condotta per i Sistemi di Informazione Creditizia (SIC): nuove disposizioni

I poteri del Garante Privacy nel GDPR

Il Garante Privacy, autorità di controllo, detiene una serie di poteri nel contesto del GDPR, tra cui indagini, azioni correttive, autorizzazioni e consulenze, oltre alla possibilità di infliggere sanzioni amministrative pecuniarie.

È diventato prioritario per ogni amministrazione **definire internamente l'ufficio responsabile dell'adeguamento al GDPR** e **designare un Responsabile del Trattamento Dati (DPO)**,

garantendo la trasparenza nel trattamento dei dati e adottando altre misure di conformità. Qui troverai una guida completa sul GDPR e la PA.

In particolare, le modifiche apportate al Codice Privacy dall'articolo 2ter del Decreto Capienze hanno esteso i poteri delle PA nel determinare la base giuridica del trattamento, non solo in base alla legge e al regolamento, ma anche attraverso atti amministrativi generali. Per ottemperare agli obblighi di conformità, le PA dovranno effettuare valutazioni interne per individuare correttamente la base giuridica e le finalità del trattamento.



Inoltre, l'abrogazione dell'articolo 2-quinquiesdecies del Codice Privacy, che consentiva al Garante Privacy di esprimere un parere preventivo per i trattamenti ad alto rischio per i diritti e le libertà degli interessati, rende le Pubbliche Amministrazioni maggiormente responsabili. Le PA dovranno assumersi il rischio di non conformità nelle scelte effettuate. Sia in termini di liceità del trattamento sia nella corretta individuazione e implementazione delle misure

di sicurezza per i trattamenti e le istruzioni operative fornite ai responsabili del trattamento. Questo è stato evidenziato nel provvedimento sanzionatorio del Garante contro Roma Capitale.

Privacy, trasparenza e GDPR: implicazioni e linee guida per il rapporto tra privacy e accesso ai documenti

Il GDPR apre **nuove prospettive sul rapporto tra privacy e trasparenza**, incluso l'ambito delle attività svolte da soggetti privati con finalità di interesse pubblico. È importante sottolineare che il regolamento non modifica direttamente le norme nazionali sull'accesso ai documenti amministrativi, ma **chiarisce l'importanza di proteggere efficacemente sia il valore della "trasparenza" che la tutela della riservatezza**.

Un'attenzione particolare è rivolta alle attività online svolte dai titolari del trattamento, specialmente alla luce dell'accelerazione digitale causata dalla pandemia. A tale proposito, l'EDPB ha emanato linee guida sui dark pattern nelle interfacce dei social media, fornendo istruzioni su come riconoscerli ed evitarli. Inoltre, l'EDPB ha creato una task force che si occupa della costruzione trasparente dei siti web e dei banner per l'installazione dei cookie.

Il GDPR introduce anche importanti novità riguardo al diritto all'oblio, in particolare nell'articolo 17. La richiesta di cancellazione dei dati personali resi pubblici da un titolare comporta l'obbligo di trasmetterla a tutti coloro che ne fanno uso. A tal proposito, l'EDPB ha elaborato linee guida sui criteri per l'esercizio del diritto all'oblio nei motori di

ricerca, indicando i motivi per cui un interessato può richiedere la deindicizzazione e le eccezioni a tale diritto.

Vantaggi strategici del GDPR: investimento essenziale per aziende e PA

L'implementazione del GDPR non deve essere considerata come un semplice costo, ma come un investimento necessario per il futuro delle imprese e delle Pubbliche Amministrazioni.

La protezione dei dati non solo assicura la conformità normativa, ma garantisce anche la qualità dei dati stessi. Un presupposto fondamentale per lo sviluppo dell'Internet delle cose e dell'intelligenza artificiale.



Uno strumento che facilita l'attuazione dei principi di tutela della privacy è il **codice di condotta per il trattamento dei**

dati personali. Ai sensi dell'articolo 40 del GDPR, le associazioni di categoria e altri organismi rappresentativi dei titolari e dei responsabili del trattamento possono redigere codici di condotta **come strumenti di autodisciplina**. Questi codici consentono di stabilire regole interne per la protezione dei dati personali, promuovendo l'uniformità all'interno di settori specifici e garantendo il rispetto delle norme del GDPR da parte dei titolari e dei responsabili.

Il controllo della conformità con un codice di condotta, come previsto dall'articolo 40, può essere effettuato da un organismo competente. Tale organismo dovrà avere le necessarie competenze sul contenuto del codice e l'accreditamento da parte dell'autorità di controllo competente, come stabilito dall'articolo 41 del GDPR. Il Garante Privacy, con il Provvedimento n.98 del 10 giugno 2020, ha approvato i requisiti di accreditamento per gli organismi di monitoraggio dei codici di condotta, previa valutazione dell'EDPB espressa il 25 maggio 2020. L'accreditamento degli organismi di monitoraggio è una condizione necessaria per l'approvazione di un codice di condotta da parte del Garante. Questi requisiti rappresentano un modello di riferimento per le associazioni che desiderano sottoporre i propri codici di condotta all'approvazione del Garante Privacy.



Linee guida per il trattamento etico dei dati personali relativi alle informazioni commerciali

Con decisione numero 127 del 12 giugno 2019, l'Autorità Garante per la protezione dei dati personali ha approvato il Codice di condotta proposto dall'Associazione Nazionale tra le Imprese di Informazioni Commerciali e di Gestione del Credito (Ancic) per il trattamento dei dati personali relativi alle informazioni commerciali. Questo nuovo Codice sostituisce il

vecchio Codice di deontologia e buona condotta per il trattamento dei dati personali a fini di informazione commerciale (Allegato A.7 del Codice Privacy). Introduce inoltre importanti miglioramenti.

Il nuovo Codice di condotta **mira a garantire una maggiore protezione delle persone coinvolte** e all'**analisi dell'impatto sulla protezione dei dati**. Mira inoltre all'**armonizzazione con le migliori pratiche europee** e l'**istituzione di un organismo di monitoraggio per le imprese aderenti** al Codice.

Il nuovo Codice di condotta sottolinea l'applicazione pratica del principio di accountability introdotto dal Regolamento Generale sulla Protezione dei Dati (GDPR). Quest'ultimo richiede alle associazioni di categoria e alle imprese di applicare consapevolmente, trasparentemente ed efficacemente le norme regolamentari.

Il nuovo testo del Codice di condotta consente alle società che forniscono informazioni sull'affidabilità commerciale di imprenditori e manager di trattare i dati personali delle persone coinvolte senza richiedere il loro consenso, basandosi sul legittimo interesse. Tuttavia, queste società devono garantire maggiori protezioni per gli interessati, fornendo loro informazioni accurate sul trattamento dei dati e garantendo l'esercizio completo dei diritti previsti dalle normative sulla privacy, come il diritto di opposizione al trattamento, di rettifica e di aggiornamento dei dati.

Misure di sicurezza e responsabilità per i fornitori aderenti

Il nuovo Codice di condotta impone ai fornitori aderenti di

adottare un approccio basato sul rischio, implementando misure tecniche, informatiche, procedurali, fisiche e organizzative per prevenire o ridurre al minimo i rischi di distruzione, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato ai dati personali.

Oltre all'osservanza delle linee guida, raccomandazioni e migliori pratiche stabilite dal Comitato europeo per la protezione dei dati (EDPB) e altre autorità competenti del settore, ogni fornitore dovrà designare, quando richiesto, un responsabile per la protezione dei dati (RPD/DPO).

Il Codice di condotta per il trattamento dei dati personali relativi alle informazioni commerciali istituisce un Organismo di monitoraggio indipendente (Odm), esterno all'Ancic, composto da individui selezionati in base a criteri di reputazione, autonomia, indipendenza e professionalità. Tale organismo sarà responsabile di verificare l'adesione al Codice di condotta da parte dei partecipanti e gestire la risoluzione dei reclami.



La versione finale del Codice di condotta è stata approvata il 29 aprile 2021, dopo essere stata modificata e integrata in conformità con la procedura di accreditamento stabilita dall'Autorità Garante. L'efficacia del Codice di condotta, approvato il 12 giugno 2019, era subordinata al completamento di tale procedura.



Codice di condotta per i Sistemi di Informazione Creditizia (SIC): nuove disposizioni

Il nuovo Codice di condotta è stato proposto dall'**Associazione Nazionale tra le Imprese di Informazioni Commerciali e di Gestione del Credito (Ancic)**. E' stato introdotto per garantire una maggiore protezione delle persone coinvolte nel trattamento dei dati personali relativi alle informazioni commerciali. Il Codice si basa sul principio di accountability introdotto dal Regolamento Generale sulla Protezione dei Dati (GDPR). Inoltre, richiede alle associazioni di categoria e

alle imprese di applicare in modo **consapevole, trasparente ed efficace** le norme regolamentari.

Il nuovo Codice consente alle società che forniscono informazioni sull'affidabilità commerciale di trattare i dati personali delle persone coinvolte senza richiedere il loro consenso, basandosi sul legittimo interesse. Queste società devono **garantire maggiori protezioni per gli interessati**, fornendo loro informazioni accurate sul trattamento dei dati. Inotre, devono garantire l'esercizio completo dei diritti previsti dalle normative sulla privacy. Il Codice di condotta richiede ai fornitori aderenti di adottare un approccio basato sul rischio e di implementare adeguate misure tecniche, informatiche, procedurali, fisiche e organizzative per prevenire o ridurre al minimo i rischi di distruzione, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato ai dati personali.

Inoltre, il Codice di condotta richiede ai fornitori di **designare un responsabile per la protezione dei dati (RPD/DPO)** quando richiesto. Questo responsabile sarà responsabile della gestione e del monitoraggio delle questioni legate alla protezione dei dati all'interno dell'organizzazione.

Per garantire il rispetto del Codice di condotta, è stato istituito un **Organismo di monitoraggio indipendente (Odm)**, esterno all'Ancic. Questo organismo sarà responsabile di verificare l'adesione al Codice di condotta da parte dei partecipanti e di gestire la risoluzione dei reclami. Il Codice di condotta è stato approvato il 29 aprile 2021, dopo essere stato modificato e integrato in conformità con la procedura di accreditamento stabilita dall'Autorità Garante. La sua efficacia era subordinata al completamento di tale procedura.

GDPR: nuovi diritti e strumenti per la tutela dei dati personali

Hanno parlato di noi

CORRIERE DELLA SERA

la Repubblica

Il Sole 24 ORE

il Giornale

ItaliaOggi

Libero Quotidiano.it

fanpage.it

PANORAMA

TGCOM24

TG5

Rai News 24









CORRIERE DELLA SERA

la Repubblica

Il Sole 24 ORE

il Giornale

ItaliaOggi



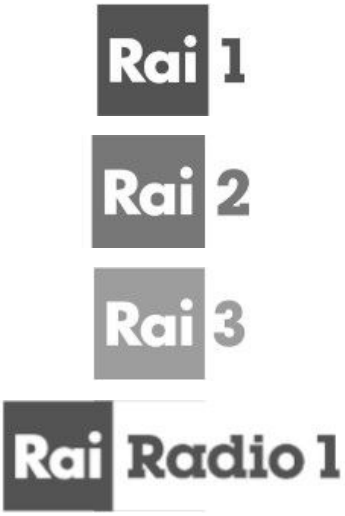
fanpage.it

PANORAMA









Contattaci

- Orari

Lunedì – Venerdì: 9.00 – 13.00 / 14.30 – 19.00

Lunedì – Venerdì:
9.00 – 13.00 / 14.30 – 19.00

- Email

info@alassistenzalegale.it

- Telefono

+39 02 5450823

Chiamaci
Contattaci

☐ Ho letto e accetto i termini dell'Informativa sulla Privacy
Invia