

Temi e questioni sul nuovo GDPR

Gli obblighi di informativa dello Studio

Cosa sta succedendo

- **Tre tappe della tutela dei dati personali**

- Direttiva comunitaria 95/46/CE
 - ha fissato i principi generali della normativa in materia di dati personali per consentire la libera circolazione dei dati personali nel territorio europeo.
- Direttive Comunitarie 2002/58/CE e 2009/136/UE
 - relative al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche hanno introdotto alcune precisazioni specifiche rispetto alla Direttiva 95/46 che riguardano la raccolta di dati personali effettuata on line e in particolare all'uso dei cookies.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016
 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che **abroga la direttiva 95/46/CE** (Regolamento generale sulla protezione dei dati).

Cosa sta succedendo

- Regolamento (UE) 2016/679
 - è stato pubblicato il 4 maggio 2016, ed è in vigore dal 25 maggio 2016.
 - Diventa pienamente operativo due anni dopo la sua pubblicazione in Gazzetta Ufficiale dell'Unione Europea quindi il **25 maggio 2018**.
 - È un **testo normativo ad efficacia differita** per permettere l'armonizzazione tra i vari ordinamenti nazionali interessati.
 - I Garanti nazionali hanno il compito di favorire l'armonizzazione tra gli stati.

Le principali novità del GDPR

- Obbligo di definire i tempi di conservazione dei dati.
- Obbligo di indicare la provenienza dei dati in caso di utilizzo.
- Obbligo di comunicare tempestivamente al Garante violazioni dei propri database.
- Obbligo di predisporre il documento di valutazione di impatto del trattamento dei dati personali.
- Obbligo di gestire l'accountability in materia di data protection con adeguati presidi organizzativi (prevalentemente mediante la nuova figura del Data Privacy Officer).

Le principali novità del GDPR

- Le regole base:
 - Trattare meno dati che puoi
 - Distribuire le responsabilità e documentare i trattamenti
 - Favorire l'anonimizzazione e la pseudonimizzazione
 - Gestire la privacy by default e by design
 - Introdurre l'accountability nella gestione dei ruoli del trattamento dei dati
 - principio di rendicontazione e responsabilità
 - il Titolare del trattamento deve
 - conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità
 - effettuare un'adeguata analisi dei rischi e documentarla

Fondamenti di liceità del trattamento

- Il regolamento **conferma** che ogni trattamento deve trovare fondamento in un'idonea **base giuridica**;
- i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy (D.Lgs. 196/2003)

Fondamenti di liceità del trattamento

- consenso
- adempimento obblighi contrattuali
- interessi vitali della persona interessata o di terzi
- obblighi di legge cui è soggetto il titolare
- interesse pubblico o esercizio di pubblici poteri
- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Consenso

- Per i dati “**sensibili**” (art. 9 GDPR) il consenso deve essere “**esplicito**”
- lo stesso dicasi per il consenso a **decisioni basate su trattamenti automatizzati** (compresa la profilazione – art. 22 GDPR).

Consenso: COSA CAMBIA?

- **Non** deve essere **necessariamente** “documentato per iscritto”, né è richiesta la “**forma scritta**”
 - anche se questa è modalità idonea a configurare l’inequivocabilità del consenso e il suo essere “esplicito” (per i dati sensibili)
 - il titolare (art. 7.1) **deve essere in grado di dimostrare che l’interessato ha prestato il consenso** a uno specifico trattamento.
- **QUINDI, MANTENIAMO LA FORMA SCRITTA O ALTRA FORMA DI PROVA DIGITALE.**

Consenso dei minori: COSA CAMBIA

- È valido a partire dai 16 anni
- prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Consenso: COSA NON CAMBIA

- Deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e **non è ammesso il consenso tacito o presunto**
 - no a caselle pre-spuntate su un modulo.
- Deve essere manifestato attraverso “**dichiarazione o azione positiva inequivocabile**”
 - (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Interesse vitale di un terzo: COSA CAMBIA

- Si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione
 - considerando 46 del GDPR

Interesse legittimo prevalente di un titolare o di un terzo: COSA CAMBIA

- Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **non spetta all'Autorità** ma **è compito dello stesso titolare**
 - si tratta di una delle principali espressioni del ***principio di "responsabilizzazione"*** introdotto dal nuovo pacchetto protezione dati.

Interesse legittimo prevalente di un titolare o di un terzo: **COSA NON CAMBIA**

- L'interesse legittimo del titolare o del terzo deve **prevalere sui diritti e le libertà fondamentali dell'interessato** per costituire un valido fondamento di liceità.
- Il regolamento chiarisce espressamente che **l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche** in esecuzione dei rispettivi compiti.

Contenuti dell'informativa: Com'è OGGI

- Art. 13 D.lgs. 196/2003.
- 1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
 - a) le finalità e le modalità del trattamento cui sono destinati i dati;
 - b) la natura obbligatoria o facoltativa del conferimento dei dati;
 - c) le conseguenze di un eventuale rifiuto di rispondere;
 - d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
 - e) i diritti di cui all'articolo 7;
 - f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

Contenuti dell'informativa: Com'è OGGI

- 2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del Codice e **può non comprendere gli elementi già noti alla persona che fornisce i dati** o la cui conoscenza può ostacolare in concreto l'espletamento, *da parte di un soggetto pubblico*, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

Contenuti dell'informativa: Com'è OGGI

- 3. Il Garante può individuare con proprio provvedimento **modalità semplificate** per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.
- 4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato **all'atto della registrazione** dei dati o, quando è prevista la loro comunicazione, **non oltre la prima comunicazione**.

Contenuti dell'informativa: Com'è OGGI

- 5. La disposizione di cui al comma 4 non si applica quando:
 - a) i dati sono trattati in base ad un **obbligo** previsto dalla **legge**, da un **regolamento** o dalla **normativa comunitaria**;
 - b) i dati sono trattati ai fini dello **svolgimento delle investigazioni difensive** di cui alla legge 7 dicembre 2000, n. 397, o, comunque, **per far valere o difendere un diritto in sede giudiziaria**, sempre che i dati siano trattati esclusivamente per tali finalità e **per il periodo strettamente necessario al loro perseguimento**;
 - c) l'informativa all'interessato comporta un impiego di mezzi **che il Garante**, prescrivendo eventuali misure appropriate, **dichiari** manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, **a giudizio del Garante**, impossibile.

Contenuti dell'informativa: Com'è OGGI

- 5-bis. L'informativa di cui al comma 1 non è dovuta in caso di ricezione di **curricula spontaneamente trasmessi** dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f).
 - Comma aggiunto dall'art. 6, comma 2, lettera a), numero 2), del decreto legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106.

Contenuti dell'informativa: COSA CAMBIA

- I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte **sono più ampi rispetto al Codice**.
- Il titolare deve **sempre** specificare
 - i dati di contatto del **RPD-DPO** (Responsabile della protezione dei dati - Data Protection Officer), **ove esistente**,
 - la base giuridica del trattamento,
 - qual è il suo interesse legittimo
 - se quest'ultimo costituisce la base giuridica del trattamento
 - se **trasferisce** i dati personali **in Paesi terzi**
 - In caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

Contenuti dell'informativa: COSA CAMBIA

- Il regolamento prevede anche **ulteriori informazioni** in quanto “necessarie per garantire un trattamento corretto e trasparente”: in particolare, il titolare
 - deve specificare **il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione**, e il diritto di presentare un reclamo all'autorità di controllo.
- Se il trattamento comporta **processi decisionali automatizzati** (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le **conseguenze** previste per l'interessato.

Tempi dell'informativa: COSA CAMBIA

- Nel caso di dati personali **non raccolti direttamente presso l'interessato** (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare **1 mese** dalla raccolta, **oppure al momento della comunicazione** (non della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente **l'art. 13, comma 4, del Codice**).

Modalità dell'informativa: COSA CAMBIA

- Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere
 - **forma concisa,**
 - **trasparente,**
 - **intelligibile** per l'interessato
 - **facilmente accessibile;**
 - occorre utilizzare un **linguaggio chiaro e semplice**
 - per i **minori** occorre prevedere **informative idonee**
 - (si veda anche considerando 58)

Modalità dell'informativa: COSA CAMBIA

- L'informativa è data, in linea di principio
 - **per iscritto**
 - preferibilmente **in formato elettronico** (soprattutto nel contesto di servizi online
 - si vedano art. 12, paragrafo 1, e considerando 58)
 - anche se sono ammessi “altri mezzi”
 - quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1).
- Il regolamento ammette, soprattutto, **l'utilizzo di icone** per presentare i contenuti dell'informativa in forma sintetica
 - **ma solo “in combinazione”** con l'informativa estesa (art. 12, paragrafo 7)
- Le icone dovranno essere **identiche in tutta l'Ue** e saranno ***definite prossimamente*** dalla Commissione europea.

Modalità dell'informativa: COSA CAMBIA

- Sono inoltre **parzialmente diversi i requisiti** che il regolamento fissa per **l'esonero** dall'informativa
 - (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo)
- Occorre sottolineare che **spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** (si veda art. 14, paragrafo 5, lettera b))
 - a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

Modalità dell'informativa: COSA NON CAMBIA

- L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento).
- Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

Modalità dell'informativa: COSA NON CAMBIA

- In tutti i casi, il titolare deve specificare
 - la propria identità
 - quella dell'eventuale rappresentante nel territorio italiano
 - le finalità del trattamento
 - i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità
 - quali sono i destinatari dei dati.
- **NOTA: ogni volta che le finalità cambiano** il regolamento impone di **informarne l'interessato** prima di procedere al trattamento ulteriore.

Diritti degli interessati: COSA CAMBIA

- Modalità per l'esercizio dei diritti
 - Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 mesi in casi di particolare complessità;
 - il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Diritti degli interessati: COSA CAMBIA

- Modalità per l'esercizio dei diritti
 - Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato,
 - ma soltanto se si tratta di **richieste manifestamente infondate** o **eccessive** (anche ripetitive) (art.12, paragrafo 5),
 - a **differenza** di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste **più "copie"** dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3);
 - in quest'ultimo caso il titolare deve tenere conto dei **costi amministrativi sostenuti**.
 - Il **riscontro** all'interessato di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità;
 - può essere **dato oralmente solo se così richiede l'interessato stesso** (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

Diritti degli interessati: COSA CAMBIA

- Modalità per l'esercizio dei diritti
 - La risposta fornita all'interessato **deve**:
 - Essere “**intelligibile**”,
 - Essere **concisa**
 - Essere **trasparente**
 - Essere **facilmente accessibile**
 - Utilizzare un **linguaggio semplice e chiaro**.

Diritti degli interessati: **COSA NON CAMBIA**

- Il titolare del trattamento deve **agevolare l'esercizio dei diritti da parte dell'interessato**
 - adottando ogni misura (tecnica e organizzativa) a ciò idonea.
- Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (art. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)).

Diritti degli interessati: COSA NON CAMBIA

- L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato,
 - possono esservi eccezioni.
- Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee
 - (si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6).

Diritti degli interessati: **COSA NON CAMBIA**

- Sono **ammesse deroghe ai diritti riconosciuti dal regolamento**, ma solo sul **fondamento di disposizioni normative nazionali**
 - ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).
- In questo senso, in via generale, possono continuare a essere applicate tutte le deroghe previste dall'art. 8, comma 2, del Codice in quanto compatibili con le disposizioni citate.
 - Al riguardo, il Garante sta valutando la piena rispondenza delle disposizioni citate in tale articolo del Codice con i requisiti fissati per la legislazione nazionale dall'articolo 23, paragrafo 2, del regolamento.

Diritto di accesso (art. 15): COSA CAMBIA

- Il diritto di accesso prevede in ogni caso il **diritto di ricevere una copia dei dati personali oggetto di trattamento.**
- Fra le informazioni che il titolare deve fornire **non rientrano le “modalità” del trattamento**, mentre **occorre indicare il periodo di conservazione previsto** o, se non è possibile, i **criteri utilizzati per definire tale periodo**, nonché **le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.**
- I titolari **possono** consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Diritto di cancellazione (diritto all'oblio) (art.17): COSA CAMBIA

- Il diritto cosiddetto “all'oblio” si configura come un diritto alla **cancellazione** dei propri dati personali **in forma rafforzata**.
- Si prevede, infatti, l'obbligo per i titolari (**se hanno “reso pubblici” i dati personali dell'interessato**: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi “qualsiasi link, copia o riproduzione” (si veda art. 17, paragrafo 2).
 - Ha un **campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice**, poiché l'interessato ha il **diritto** di chiedere la **cancellazione** dei propri dati, per esempio, **anche dopo revoca del consenso** al trattamento (si veda art. 17, paragrafo 1).

Diritto di limitazione del trattamento (art. 18): COSA CAMBIA

- Si tratta di **un diritto diverso e più esteso rispetto al “blocco”** del trattamento di cui all’art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile
 - non solo in caso di **violazione dei presupposti di liceità del trattamento** (quale alternativa alla cancellazione dei dati stessi)
 - **anche se l’interessato chiede la rettifica dei dati** (in attesa di tale rettifica da parte del titolare) **o si oppone al loro trattamento** ai sensi dell’art. 21 del regolamento (in attesa della valutazione da parte del titolare).
- **In che consiste: Esclusa la conservazione, ogni altro trattamento** del dato di cui si chiede la limitazione **è vietato** a meno che ricorrano determinate circostanze
 - (consenso dell’interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Diritto alla portabilità dei dati (art. 20): COSA CAMBIA

- Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).
- Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei)
- Sono previste specifiche condizioni per il suo esercizio;
 - sono portabili solo i dati trattati con il consenso dell'interessato
 - sulla base di un contratto stipulato con l'interessato
 - solo i dati che siano stati "forniti" dall'interessato al titolare (si veda il considerando 68 per maggiori dettagli).
 - (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio),
- Il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Ma insomma, che si deve fare?

- Un percorso ideale
 - Modello di raccolta dati
 - Preventivo
 - Incarico

Maggiori dettagli: <http://www.garanteprivacy.it/regolamentoue>

Webgrafia: www.garanteprivacy.it