Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Regolamento Privacy UE in 6 punti. Le Linee Guida del Garante Privacy

di Deborah Bianchi

Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Le *Linee Guida del Garante Privacy* 28.04.2017 tentano una sintesi esplicativa del Regolamento Privacy UE in 6 punti toccando i seguenti temi principali: Fondamenti di liceita' del trattamento; Informativa; Diritti Interessato; Ruoli Privacy (Titolare, Responsabile, Incaricato); Approccio "risk-based" e misure di accountability (Registro dei trattamenti, Data Privacy Officer, Notifica Data Breach); Trasferimento dati all'Estero. Uniti a ciascuna scheda vengono elargiti preziosi consigli denominati Raccomandazioni volti a preparare il Titolare nell'applicazione della nuova disciplina europea sulla privacy. In particolare, **al fine di apportare le modifiche o le integrazioni eventualmente necessarie prima del 25 maggio 2018** (data di efficacia del GDPR 2016/679) le Linee Guida "raccomandano" ai Titolari di verificare la rispondenza delle Informative attualmente utilizzate alle nuove regole europee con particolare riguardo ai contenuti obbligatori e alle modalità di redazione.

FONDAMENTI DI LICEITA' DEL TRATTAMENTO O BASE GIURIDICA

(Art. 6 GDPR 2016/679)

L'art. 6 del GDPR 2016/679 individua i fondamenti di liceità del trattamento ovvero gli elementi atti a giustificare il trattamento dei dati. Tali figure vengono denominate dal Regolamento UE *"fondamenti"* o "*base giuridica*" e si sostanziano nel **consenso**; nel **contratto**; nella **legge** (obbligo legale cui è sottoposto il Titolare); nell'**interesse vitale** dell'interessato o di un terzo; nell'**interesse legittimo prevalente**; nei compiti di **interesse pubblico** cui è tenuto il titolare.
Le Linee Guida, una volta osservato che si tratta degli stessi fondamenti stabiliti dal nostro Codice Privacy, si soffermano in particolare sull'analisi del consenso, dell'interesse vitale e dell'interesse legittimo prevalente.

Il consenso è uno dei principali fondamenti di liceità del trattamento. Il confronto tra l'attuale Codice Privacy e il Regolamento UE 2016/679 non scalfisce il primato del consenso quale istituto legittimante del trattamento. Esistono solo piccole differenze normative. Nei trattamenti ad alto rischio (es.: dati sensibili, profilazione, trasferimento all'Estero) sul tema della modalità di espressione del consenso, la visione rigoristica del Codice richiede la forma scritta mentre il Regolamento UE richiede che il consenso sia *"esplicito"* e "*dimostrabile*". La forma scritta è l'unica che garantisce in toto la possibilità di "*dimostrare*" l'*"esplicito"* consenso dell'interessato e così – in sostanza – anche la disciplina europea richiede al Titolare di procurarsi il consenso in forma scritta o comunque con manifestazione volitiva inequivocabile come apporre un flag su una casella. Nel Regolamento UE esistono poi delle nuove figure di consenso dovute a scenari digitali che all'epoca del Codice (2003) non esistevano come ad esempio i trattamenti automatizzati o i trattamenti dati dei minori. Un'attenta disamina della figura privacy "Consenso" nel Regolamento UE individua distintamente componenti codicistiche restate in piedi accanto a componenti nuove introdotte dal legislatore europeo. Così in termini non del tutto ortodossi, potremmo osservare che l'integrazione tra la fonte normativa interna e la fonte europea ci consegna la **figura di consenso applicabile.** L'analisi

integrata dell'articolato delle due discipline esposta di seguito sarà in grado di svelare quali parti del Consenso codicistico restano in vita nel Regolamento europeo; quali parti costituiscono novità introdotte dal legislatore UE; come si presenta la nuova figura privacy del Consenso derivante dall'integrazione delle due componenti normative (disciplina precedente e disciplina attuale).

Analisi integrata dell'articolato:

Art. 23 Codice Privacy
Consenso dev'essere informato, libero e specifico. Per i dati sensibili il consenso dev'essere scritto. Non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate).
Art. 9 GDPR 2016/679
Consenso dev'essere informato, libero e specifico. Per i dati sensibili il consenso dev'essere esplicito. Non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate).
Art. 22 GDPR 2016/679
Occorre consenso esplicito per trattamenti automatizzati (es.: profilazione).
Art. 49 GDPR 2016/679
Occorre consenso esplicito per il trasferimento di dati all'Estero o a organizzazioni internazionali.
Art. 8 GDPR 2016/679
Consenso del Minore è valido solo a partire dai 16 anni. In difetto occorre consenso esplicito dei genitori.
Art. 7 (2) GDPR 2016/679
La richiesta di consenso dev'essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato nei moduli contrattuali.
Art. 7 (1) GDPR 2016/679
Il Titolare dev'essere in grado di dimostrare il consenso e quindi il suggerimento è quello di richiedere il consenso - nei casi dovuti - sempre in forma scritta come stabilito nel Codice Privacy o comunque con manifestazione volitiva inequivocabile come l'apposizione di flag..
Considerando 32 GDPR 2016/679
Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

CONSENSO

Il consenso applicabile secondo il Regolamento UE dev'essere:

- informato, libero e specifico;
- chiaramente distinguibile;
- nè tacito, nè presunto (no a caselle pre-spuntate);
- in forma scritta o inequivocabile per i dati sensibili, i trattamenti automatizzati, i trasferimenti all'Estero;
- valido per i minori a partire dai 16 anni;
- richiesto in modo chiaro, conciso e non interferente col servizio selezionato quando avviene tramite Internet.

Dall'integrazione di tutte queste norme deriva la nuova figura di Consenso.

Interesse vitale dell'Interessato o di un Terzo. L'interesse vitale - sebbene inquadrato quale fondamento di liceità del trattamento – costituisce tuttavia una fattispecie residuale che viene ammessa dal Considerando 46 GDPR 2016/679.quando *"il trattamento non può essere manifestamente fondato su un'altra base giuridica"* come nei casi di soccorso umanitario richiesto a causa di eventi catastrofici.

Interesse legittimo prevalente di un Titolare o di un Terzo. L'interesse legittimo prevalente rappresenta la valvola di sicurezza del "sistema privacy" in quanto idoneo a risolvere i conflitti tra Titolare e Interessato oppure tra Interessato e Terzi.
Pensiamo ad esempio al Provvedimento del nostro Garante Privacy 19 gennaio 2017 [6068256] sul caso Ikea http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/6068256
Qui l'Interessato è cliente del Titolare (Ikea) che adotta misure antifrode ubicate su server americani per evitare illeciti nelle vendite e-commerce.
Si tratta innanzitutto di un trasferimento dati all'Estero (USA) necessitante del consenso dell'interessato che risulta oltremodo gravoso ottenere perché dovrebbe essere espresso per ogni transazione eseguita.
Si tratta altresì di un trattamento incrociato di dati personali del cliente. Il sistema di vendita e-commerce della piattaforma Ikea trasmette al sistema antifrode i dati della transazione (ammontare della somma autorizzata, identificativo della transazione), i dati del customer host (nome, cognome, indirizzo e-mail, indirizzo civico, indirizzo IP), i dati della spedizione, i dati relativi alla modalità di accesso (es. cliente registrato o ospite, privato o azienda), i dati dell'acquisto (nome e prezzo del prodotto). Il sistema antifrode allocato su server USA procede a verificare queste informazioni con parametri quali "*congruità tra luogo di emissione della carta e indirizzo IP da dove giunge la richiesta di transazione; numero degli acquisiti eseguiti nella giornata dalla stessa carta; valore totale degli acquisti; nome dell'acquirente privo di vocali; provenienza da domini storicamente etichettati come non sicuri; controlli su indirizzi diversi usati per pagamenti con la stessa carta; coerenza fra i dati della carta e quelli relativi alle transazioni precedenti; numero di pagamenti in un periodo di tempo predeterminato; verifiche su eventuali tentativi di acquisto con numeri di carta sequenziali".* Alla fine di tutte queste operazioni automatizzate l'intelligenza artificiale decide se autorizzare o meno la transazione.
Da una parte abbiamo questo sistema antifrode che implica molti trattamenti rischiosi necessitanti del consenso del cliente-Interessato come ad esempio il trasferimento dati all'Estero, la verifica incrociata dei dati, le operazioni automatizzate guidate da intelligenza artificiale. **Dall'altra parte** abbiamo l'enorme difficoltà del Titolare-Ikea a ottenere il consenso per ogni transazione. **Cosa fare? A quale posizione dare prevalenza: all'Interessato o al Titolare?**
L'unico modo per risolvere la questione si sostanzia nell'applicazione del **bilanciamento delle posizioni contrapposte** secondo criteri di **proporzionalità**. Il Garante, verificato che il sistema americano antifrode risulta impostato secondo principi di minimizzazione nell'utilizzo delle informazioni o cosiddetti *privacy by design*, decide che non costituisce un sacrificio sproporzionato per l'Interessato essere sottoposto a tale sistema. Si noti inoltre che l'interesse economico del Titolare Ikea non solo non infligge un peso troppo gravoso ma coincide anche con l'interesse pubblico a evitare furti di identità ai danni dei clienti. All'esito di tali ponderazioni il Garante - dopo avere aggiustato il tiro con ulteriori misure di sicurezza - conclude che **è giusto elevare l'interesse privato** di Ikea **a interesse legittimo.** Interesse legittimo che secondo Garante Privacy 19 gennaio 2017 [6068256] *"ai sensi dell'art. 24, comma 1, lett. g), del Codice, individua nel trattamento di dati per finalità antifrode un'ipotesi in cui non è richiesto il consenso degli interessati"*

oppure Interesse legittimo che secondo il Regolamento UE costituisce "*base giuridica*" legittimante il trattamento.

Bilanciamento nel Regolamento UE viene eseguito dal Titolare del trattamento. Questa novità del legislatore europeo rispecchia perfettamente uno dei filoni portanti della nuova disciplina privacy ovvero il filone della cosiddetta **"accountability"** secondo cui il Titolare deve contemporaneamente sentirsi fortemente responsabilizzato nelle proprie decisioni di privacy governance e ricercare i metodi per dimostrare di avere assunto adeguate misure di contrasto al rischio data protection.

INFORMATIVA

(Artt.13 e14 GDPR 2016/679)

Nell'era dei Big Data e dei Data Analytic, il diritto all'autodeterminazione informativa elettronica o diritto alla privacy o diritto Data Protection assume una funzione di tutela della persona ancora più pregnante. Se finora l'obiettivo perseguito era quello di garantire il diritto alla conservazione dell'attualità dell'identità digitale, adesso abbiamo l'obiettivo ulteriore di proteggere la persona da etichettature di massa derivate da trattamenti automatizzati. Pensiamo a un Interessato sottoposto a una *"decisione basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani"* (Considerando 71 e artt. 17,21-22 GRDP 679/2016).
L'interessato ha il **diritto alla trasparenza** sulle modalità di trattamento assunte e **l'Informativa costituisce lo strumento principe** per garantire questo valore.
L'Informativa nel Regolamento Ue viene disciplinata secondo tre ambiti: i **contenuti**, i **tempi**, le **modalità**.

Informativa. I contenuti.
I contenuti dell'Informativa prevista dal Regolamento UE coincidono con quelli della versione codicistica con l'aggiunta di qualche novità come l'obbligo di indicare ulteriori elementi quali la base giuridica del trattamento oltre alle finalità; gli identificativi del Responsabile della protezione dei dati o DPO ove esistente; le eventuali ipotesi di trasferimento dati all'Estero; le eventuali ipotesi di processi automatizzati come la profilazione esplicando la logica che li governa; il periodo o i criteri di conservazione.
Abbiamo già tentato con il Consenso la ricostruzione di una figura privacy a partire dall'integrazione della normativa codicistica interna (recepita dal legislatore europeo) con quella del Regolamento UE. In definitiva ci siamo chiesti: quali parti del Consenso codicistico restano in vita nel Regolamento europeo? Quali parti costituiscono novità introdotte dal legislatore UE? Come si presenta la nuova figura privacy del Consenso derivante dall'integrazione delle due componenti normative (disciplina precedente e disciplina attuale)?
Proviamo di seguito ad eseguire la stessa analisi per la figura privacy dell'Informativa.

Analisi dell'articolato:

Art. 13 Codice Privacy

L'Informativa deve tassativamente contenere le seguenti indicazioni:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le possibili conseguenze di un eventuale rifiuto di rispondere;
- 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;
- i diritti dell'Interessato di cui all'articolo 7;
- gli estremi identificativi del Titolare e, se designato, del relativo Rappresentante nel territorio dello Stato nonché gli estremi identificativi - ove nominato - del Responsabile per il riscontro all'interessato.

Art. 13 GDPR 2016/679 (dati ottenuti presso l'Interessato)

L'Informativa deve tassativamente contenere le seguenti indicazioni:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del Responsabile della protezione dei dati o DPO (Data Privacy Officer), ove previsto;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- i diritti dell'Interessato (accesso, rettifica, cancellazione, revoca, limitazione del trattamento, portabilità, opposizione, reclamo);
- l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
- periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- le possibili conseguenze di un eventuale rifiuto di fornire i dati ove l'Interessato sia obbligato;
- l'esistenza di un processo decisionale automatizzato (es.: profilazione) e la logica che lo governa nonché le possibili conseguenze di siffatto trattamento;
- obbligo del Titolare di fornire una nuova Informativa ad hoc ove decida di trattare i dati in suo possesso per finalità differenti da quelle per cui quegli stessi dati sono stati raccolti.

Art. 14 GDPR 2016/679 (dati non ottenuti presso l'Interessato)

L'Informativa deve tassativamente contenere oltre a tutto quanto già disposto nell'art. 13 GDPR 2016/679 anche le seguenti indicazioni:

- le categorie di dati trattati;
- la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
- ipotesi di esonero dall'Informativa quando l'Interessato dispone già delle informazioni oppure quando comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato.

Dall'integrazione di tutte queste norme derivano i Contenuti della nuova figura di Informativa.

INFORMATIVA. I CONTENUTI.

I contenuti dell'Informativa secondo il Regolamento UE devono essere:

- estremi identificativi del Titolare, del relativo Rappresentante nel territorio dello Stato, del Responsabile designato al riscontro, del Data Privacy Officer ove previsto;
- finalità e modalità del trattamento;
- base giuridica del trattamento;
- interesse legittimo prevalente ove previsto quale base giuridica;
- categorie di dati trattati;
- fonte da cui hanno origine i dati ottenuti ove raccolti da soggetto diverso dall'Interessato;
- natura obbligatoria o facoltativa del conferimento dei dati;
- possibili conseguenze del rifiuto;
- soggetti ai quali i dati personali possono essere comunicati in qualità di Responsabile o in qualità di Destinatario;
- diritti dell'Interessato: accesso, rettifica, cancellazione, revoca, limitazione del trattamento, portabilità, opposizione, reclamo;
- ipotesi di trasferimento dati all'Estero;
- ipotesi di trattamento automatizzato;
- ipotesi di nuovi trattamenti e obbligo nuova Informativa ad hoc;
- tempi o criteri di conservazione;
- ipotesi di esonero dall'Informativa.

Informativa. I tempi.

I tempi dell'Informativa attengono a due ipotesi:

- nel caso dei **dati ottenuti da soggetto diverso dall'Interessato** ex art. 14, (3) GDPR 2016/679, il Titolare deve fornire l'Informativa entro 1 mese dalla raccolta oppure alla prima comunicazione all'Interessato o ancora non oltre la prima comunicazione al terzo destinatario;
- nel caso di **richiesta dell'Interessato in merito ai propri diritti** ex art. 12, (3) GDPR 2016/679, il Titolare deve fornire riscontro entro 1 mese dall'istanza estensibile fino a 3 mesi ove trattasi di ipotesi particolarmente complesse. Il Titolare deve rispettare lo stesso termine di 1 mese anche per comunicare all'Interessato le motivazioni per cui non intende ottemperare e la possibilità di impugnare tale decisione con reclamo o con ricorso al giudice.

Informativa. Le modalità.

Le modalità dell'Informativa – già in più casi indicate dal Garante nostrano in alcuni provvedimenti - vengono razionalizzate in modo compiuto dall'art. 12 del Regolamento europeo.

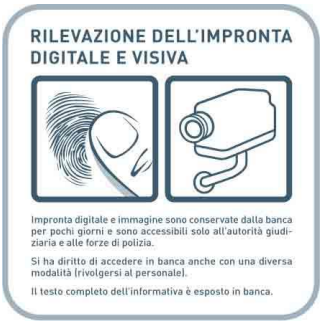
Questa disposizione richiede:

- forma **concisa**, **trasparente**, **intelligibile** e facilmente **accessibile**;
- **linguaggio semplice e chiaro** in particolare per l'**Informativa ai Minori**;
- forma **scritta** oppure forma **elettronica;**
- **possibilità di "Informativa stratificata"** (Informativa base combinata con Informativa estesa).

Occorre puntualizzare meglio l'ipotesi dell'Informativa resa in **forma stratificata** in quanto fortemente caldeggiata dal Regola mento UE per le proprie caratteristiche di semplicità e immediatezza. Si tratta di un'Informativa costituita di due componenti: una componente base idonea a fornire l'essenziale e una componente estesa in cui si legge la versione integrale dell'Informativa. Il Legislatore europeo avverte che non è ammesso utilizzare la forma base scissa dalla forma estesa in quanto verrebbero meno delle garanzie informative dedicate all'utente. La combinazione tra componente base e componente estesa avviene tramite un rimando che collega le due versioni. Nell'ambiente materico-analogico l'utente vede un cartello illustrativo in cui si legge che per approfondire si possono trovare le informazioni complete in un prospetto esposto in bacheca. Nell'ambiente elettronico-digitale l'utente vede un'icona supportata da breve delucidazione che rimanda tramite link al testo integrale dell'Informativa.

Un esempio calzante di **"Informativa stratificata"** si individua nel Provvedimento Garante Privacy "*Rilevazione di impronte digitali ed immagini per accedere agli istituti di credito: limiti e garanzie - 27 ottobre 2005"* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675

Qui vengono valutate le misure privacy per il trattamento dati ai fini dell'accesso alla filiale bancaria. L'Authority invita l'istituto di credito-Titolare ad affiggere in prossimità della zona sottoposta a sorveglianza video e a rilevamento impronte digitali un cartello contenente la figura (icona) della videocamera e dell'impronta accompagnate dal seguente testo: *"Rilevazione dell'impronta digitale e visiva. Impronta digitale e immagine sono conservate dalla banca per pochi giorni e sono accessibili solo all'autorità giudiziaria e alle forze di polizia. Si ha diritto di accedere in banca anche con una diversa modalità (rivolgersi al personale). Il testo completo dell'informativa è esposto in banca".*



Il Regolamento UE promuove fortemente l'utilizzo dell'**"Informativa stratificata" con icone** nell'ambiente Internet in quanto ideale per garantire la massima diffusione e semplificare la prestazione delle informative. Nell'attesa che la Commissione UE stabilisca delle icone standardizzate valide per tutti gli Stati Membri, è possibile utilizzare le icone dell'Authority interna già coniate nei vari provvedimenti come quelle per la videosorveglianza o per le banche.

Un'ipotesi di **"Informativa stratificata elettronica" con icone** potrebbe essere composta secondo lo schema seguente.

INFORMATIVA PRIVACY

I Tuoi dati personali e/o sensibili e/o giudiziari e/o medici o di salute quale Interessato-privacy saranno trattati, manualmente ed elettronicamente, da NOME TITOLARE - titolare del trattamento - così come descritto nella nostra Privacy policy che viene resa disponibile on line sul nostro sito web (**LINK A PRIVACY POLICY**). NOME TITOLARE Codice Fiscale XXXXXXX nella persona del legale rappresentante pro tempore e con sede legale in INDIRIZZO – e-mail: info@nometitolare.it; PEC pec@nometitolare.it è il Titolare del trattamento e utilizza i Tuoi dati secondo le finalità stabilite dalla disciplina INSERIRE BASE GIURIDICA.

NOME TITOLARE garantisce all'interessato che per qualsiasi trattamento il principio assunto è quello della **minimizzazione** e che i suoi dati verranno utilizzati e **conservati** solo quando siano indispensabili per svolgere attività (istituzionali o aziendali a seconda del tipo di titolare) che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. Comunque i dati personali e/o sensibili e/o giudiziari e/o sanitari vengono cancellati non appena esaurita la finalità del relativo utilizzo.

Il titolare dichiara che **non vengono eseguiti trattamenti automatizzati o di profilazione** dei dati personali conferiti. Attualmente non è previsto **nessun trasferimento dei dati personali all'Estero** (Paesi ExtraUE).

In caso di perdita dei dati dell'interessato (caso del **Data Breach**), NOME TITOLARE provvederà a darne immediatamente comunicazione a quest'ultimo e alle competenti Autorità.

Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

DIRITTI DEGLI INTERESSATI

(Artt.12, 13,14, 15, 16, 17, 18, 20 e 21 GDPR 2016/679)

I Diritti dell'Interessato stabiliti dal Regolamento Ue riprendono tutti quelli già previsti dal Codice Privacy (escluso il diritto al blocco dati sostituito con il più ampio diritto alla limitazione del trattamento) aggiungendo qualche novità.

L'Interessato ha diritto di **sapere, chiedere, reclamare, ricorrere, opporsi.**

SAPERE

L'Interessato **ha diritto di sapere:**

- **quali** dei propri **dati** sono presenti nella struttura del Titolare (**diritto di accesso**) con possibilità di ottenerne una copia (la richiesta di più di una copia implica il pagamento dei costi amministrativi);
- **per quanto tempo saranno conservati o secondo quali criteri;**
- **quali garanzie** vengono offerte in caso di **trasferimento** dei propri dati **all'Estero.**

  L'Interessato per avere queste informazioni può scrivere una e.mail al Responsabile del riscontro designato dal Titolare che dovrà rispondere **entro 1 mese** estensibile a 3 mesi nei casi di maggiore complessità. Il Titolare deve rispondere entro 1 mese anche se decide di non ottemperare e ne fornisce le motivazioni indicando la possibilità di reclamare o di ricorrere.

  Il riscontro **è gratuito** salvo i casi di richieste manifestamente infondate o eccessive o ripetitive. In queste ultime ipotesi il Titolare è autorizzato a stabilire l'ammontare dell'**eventuale contributo**. In merito l'art. 70 del Regolamento con riguardo ai compiti del Comitato prevede la possibilità che quest'ultimo possa definire linee-guida specifiche di concerto con le altre autorità Ue.

  La risposta fornita all'Interessato deve essere **concisa**, **trasparente** e facilmente **accessibile**, oltre a utilizzare un linguaggio semplice e chiaro. Inoltre è obbligatorio per il Titolare fornire tale riscontro in **forma scritta** anche elettronica.

  Inoltre secondo il Considerando 68 del Regolamento UE il Titolare potrebbe allestire **un'area riservata** on line dove l'Interessato possa attingere le informazioni di cui necessita da remoto in modo sicuro.

CHIEDERE

L'Interessato **può chiedere** direttamente **al Titolare:**

- La correzione delle informazioni che lo riguardano quando sono state raccolte in modo errato (**diritto di rettifica**);
- L'aggiornamento delle informazioni che lo riguardano quando non sono più attuali (**diritto di rettifica**);
- L'integrazione delle informazioni che lo riguardano quando sono state raccolte in modo incompleto (**diritto di rettifica**);

- La trasformazione in forma anonima delle informazioni che lo riguardano quando non sono più necessarie per le finalità di trattamento esposte nell'informativa dal Titolare (**diritto all'anonimizzazione** dei dati);
- La cancellazione delle informazioni che lo riguardano quando il Titolare non ha più nessuna ragione per conservarle nella propria struttura (**diritto alla cancellazione**);
- L'oblio - ovvero l'oscuramento sul web - delle informazioni che lo riguardano quando il Titolare non ha più nessuna ragione per conservarle e nonostante ciò continua a diffonderle on line e a renderle indicizzabili dai motori di ricerca (**diritto alla cancellazione**). Si noti che questo diritto risulta **rafforzato rispetto alla versione codicistica** in quanto il Titolare è obbligato a informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" ex art. 17, (2) DPR 2016/679;
- La limitazione del trattamento perchè ad esempio alcuni dati sono in eccesso rispetto alle finalità da espletare (**diritto alla limitazione** del trattamento). Si noti che questo diritto risulta **molto più ampio e flessibile** rispetto al diritto al **blocco** dei dati della versione codicistica in quanto è esercitabile non solo quale alternativa alla cancellazione bensì anche quale rimedio temporaneo in attesa dell'esecuzione della rettifica o in attesa della decisione a seguito di opposizione;
- La portabilità dei propri dati dal Titolare a un altro Titolare senza nessun costo aggiuntivo e senza nessuna lungaggine burocratica (**diritto alla portabilità**). Si tratta di uno dei nuovi diritti previsti dal Regolamento UE che all'uopo prescrive ai Titolari di produrre i dati richiesti in un **formato interoperabile** in modo che il trasferimento da una piattaforma digitale all'altra sia tecnicamente agevole (Considerando 68 GDPR 2016/679 e "*Linee-guida sul diritto alla portabilità dei dati*" del Gruppo "Articolo 29").

  Il Gruppo dei **Garanti Privacy UE** o WP29 si è preoccupato delle eventuali ipotesi di conflitto tra i diritti dei terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilità. A tal riguardo si vedano le ***"Linee-guida sul diritto alla portabilità dei dati"*** del 13.12.2016 redatte dal WP29 nella versione emendata e adottata il 5 aprile 2017 al seguente link: http://194.242.234.211/documents/10160/5184810/Linee-guida+sul+diritto+alla+portabilit%C3%A0+dei+dati+-+WP+242.pdf;
- L'**attestazione** che le **operazioni richieste sono state portate a conoscenza**, anche per quanto riguarda il loro contenuto, **di coloro ai quali i dati sono stati comunicati** eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

RECLAMARE

L'Interessato – se il Titolare non risponde o non fornisce una risposta convincente - **può rivolgersi al Garante Privacy:**

- mediante formale **Reclamo** in cui vengono esposti i motivi di disaccordo con il Titolare del Trattamento secondo le istruzioni visionabili sul sito del Garante Privacy.

RICORRERE

L'Interessato – se il Titolare non risponde, non fornisce una risposta convincente o se la decisione del Garante Privacy non risulta soddisfacente - **può rivolgersi al Giudice:**

- mediante una vera e propria **Causa** nei confronti del Titolare del Trattamento;
- mediante una **Impugnazione** della decisione emessa nei confronti del Garante Privacy.

OPPORSI

L'Interessato – mediante comunicazione al Titolare del Trattamento - **può decidere** di:

- presentare **Opposizione** al trattamento per motivi legittimi;
- **Revocare** il consenso al trattamento che aveva concesso precedentemente.

TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

(Artt. 24,25,26,27,28,29,30,32 e 37 GDPR 2016/679)

I Ruoli Privacy previsti dal **Regolamento UE** coincidono quasi tutti con quelli del Codice Privacy salvo l'eccezione del **sub-responsabile**, dell'incaricato codicistico che nel testo europeo diventa la "***persona autorizzata al trattamento*** *dei dati personali sotto l'autorità diretta del titolare o del responsabile*" (art. 4, GDPR 679/2016) e l'eccezione del Responsabile della protezione dei dati o **Data Privacy Officer** inesistente nella precedente disciplina. In questa sede ci limitiamo a sottolineare soltanto la particolarità del **nuovo regime di responsabilità nel sistema-privacy.**

Questo nuovo sistema di responsabilità coinvolge la figura del Responsabile, del Titolare e del sub-responsabile. In particolare i primi due soggetti privacy ripartiscono i rispettivi rischi tramite un contratto che potremmo definire "Contratto di ripartizione del rischio privacy".

Contratto di ripartizione del rischio privacy.

La **novità** assoluta del legislatore europeo oltre all'introduzione del DPO si sostanzia nel diverso regime di responsabilità posto in capo al Responsabile del trattamento. Mentre nella disciplina codicistica il Responsabile si atteneva alla lettera di incarico del Titolare senza assumere responsabilità nei confronti dei terzi adesso invece assurge a **contitolare della responsabilità** verso l'esterno e quindi ha una posizione molto più rischiosa rispetto alla precedente. Del resto anche la posizione del Titolare cambia nel rapporto con il Responsabile in quanto dovrà preoccuparsi di stipulare un vero e proprio **contratto di ripartizione del rischio privacy** con i propri Responsabili

Questo tipo di accordo deriva da uno dei principi fondanti del Regolamento UE ovvero il principio di **"accountability"** o responsabilizzazione secondo cui Titolari e Responsabili devono stabilire e dimostrare l'adozione di misure atte a garantire proattivamente l'osservanza della nuova disciplina. A tal fine sarebbe importante l'adozione di **Codici di Condotta** virtuosi che possano fornire in un certo qual modo la **certificazione** di avere assunto una condotta responsabile o meglio una condotta "accountability addicted" come indicato dall'art. 28 (5) GDPR 679/2016.

Il **contratto di ripartizione del rischio privacy** deve disciplinare **tassativamente**:

- le **materie riportate** al paragrafo 3 dell'**art. 28 GDPR 2016/679** al fine di dimostrare che il responsabile **fornisce "garanzie sufficienti"** al Titolare di avere adottato misure di sicurezza adeguate al livello di protezione stabilito con il Titolare e stabilito dal Regolamento europeo;
- in particolare, la **natura**, **durata** e **finalità** del trattamento o dei trattamenti assegnati, le **categorie di dati** oggetto di trattamento, le **misure tecniche e organizzative** adeguate.

La Commissione e i Garanti nazionali stanno valutando la possibilità di redigere delle clausole contrattuali modello da utilizzare appositamente per il contratto di ripartizione del rischio privacy.

Responsabile e sub-responsabile.

Il Responsabile ha degli obblighi specifici distinti da quelli del Titolare. In particolare rientra tra gli **obblighi specifici del Responsabile**:

- la tenuta del **Registro dei trattamenti** ex art. 30 (2) GDPR 2016/679;
- l'adozione di **idonee misure** tecniche e organizzative per garantire la sicurezza dei trattamenti ex art. 32 GDPR 2016/679;
- la **designazione di un RPD-DPO**, nei casi previsti ex art. 37 GDPR 2016/679;
- la **designazione di un rappresentante in Italia** quando ricorrono le condizioni da parte del Responsabile non stabilito nell'Ue.

Il sub-responsabile.

Il sub-responsabile viene nominato dal Responsabile **-** previo ottenimento autorizzazione da parte del Titolare - per **specifiche attività** di trattamento e nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario. La condotta del sub-responsabile viene coperta dalla figura del **Responsabile** che **risponde personalmente** dinanzi al titolare degli inadempimenti del sottoposto privacy anche ai fini del risarcimento del danno, salvo la prova che l'evento dannoso "*non gli è in alcun modo imputabile*" ex art. 82, (1) e (3) GDPR 2016/679.

APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI

(Artt. 24,25,26,27,28,29,30,32,35,36 e 37 GDPR 2016/679)

La figura preponderante del sistema privacy disegnato dal Regolamento Ue è costituita dal Rischio. La preoccupazione del **rischio di sinistro** ai danni dei diritti dell'Interessato (Considerando 75-77 GDPR 2016/679) **deve guidare i processi di Data Protection Governance adottati dal Titolare**. Infatti le Linee Guida parlano di un approccio "risk-based" tentando di illustrarlo per sommi capi.

Approccio "risk-based".

La procedura per stabilire le soglie di rischio presenti nella struttura da regolamentare implica due fasi fondamentali: la valutazione di impatto privacy (PIA) e l'eventuale Consultazione preventiva dell'Authority interna.

Valutazione d'impatto sulla protezione dei dati ex art. 35 GDPR 679/2016.

La valutazione deve considerare e pre-ipotizzare l'eventuale impatto negativo dei trattamenti in esecuzione sulle libertà e i diritti degli interessati.

- **Censimento della struttura.** A tal fine occorre fare il censimento della propria struttura in modo da acquisire la cognizione piena della propria organizzazione interna ed esternalizzata a livello materiale, elettronico e di risorse umane. Occorre inoltre sapere quali trattamenti vengono eseguiti e da quali operatori.
- **Mappatura dei trattamenti e Organigramma Ruoli Privacy.** Una volta fatto il censimento e possibilmente redatto una mappatura dei trattamenti e un organigramma dei ruoli privacy, il Titolare è in grado di verificare l'esistenza di eventuali falle del sistema. Può darsi che si evincano dei trattamenti mancanti di adeguata copertura del personale oppure addirittura curati da molteplici operatori.
- **Misure idonee a mitigare il rischio-privacy.** Sia nella prima che nella seconda ipotesi si registra un rischio sicurezza perché nessuno si occupa della protezione di quei dati o perché se ne occupano in troppi attivando una sovrapposizione di ruoli non corrispondente all'incarico conferito. In questo caso il rischio attiene al profilo organizzativo e quindi il rimedio applicabile risiede nell'adozione di **misure logico-organizzative** come la redazione di lettere di incarico precise "su chi fa che cosa".
  Altre volte si possono registrare delle carenze nel sistema informatico e informativo della struttura perché essendo un po' vecchio risulta incapace di lavorare applicando l'anonimizzazione dei dati o comunque la minimizzazione del relativo utilizzo. In questo caso il rischio attiene al profilo tecnico e quindi il rimedio sarebbe implementare nella struttura delle nuove attrezzature informatiche dotate di sistemi di **"privacy by default" o "privacy by design".** Si tratta di sistemi operativi informatici che, per impostazione predefinita, utilizzano solo i dati personali necessari (art. 25 (2), GDPR 2016/679).
- **Bilanciamento rischi, costi e benefici.** All'esito di questa valutazione il Titolare decide di adottare le misure di contrasto più urgenti e necessarie alla propria struttura **compatibilmente con il livello di rischio registrato** (lieve, medio, alto) **e con le proprie risorse economiche**. Il Legislatore europeo sottolinea infatti che non è possibile pretendere un adeguamento privacy totalizzante e **lascia al Titolare, responsabilizzandolo fortemente, il compito di bilanciare** rischi, costi e benfici in relazione alla propria situazione.

Consultazione preventiva presso Authority ex art. 36 GDPR 679/2016.

Ove il Titolare non si reputi in grado di farlo, può rivolgersi al Garante Privacy interno e richiedere una Consultazione preventiva ai sensi dell'art. 36 GDPR 2016/679.

Questo procedimento tuttavia non deresponsabilizza il Titolare che comunque deve presentare il proprio piano di adeguamento privacy. L'autorità non ha il compito di "autorizzare" il trattamento ma interviene ex post per indicare misure aggiuntive rispetto a quelle già stabilite dal Titolare.

Il Regolamento UE **abolisce** la **Notifica preventiva al Garante e** la procedura del **Prior Checking** o Verifica preliminare ex art. 17 Codice Privacy **sostituendola** con l'obbligo (solo nei casi stabiliti) di tenere il **Registro dei Trattamenti** che implica la **responsabilità** di determinare il piano di adeguamento privacy sulla scorta della PIA e del bilanciamento rischi, costi, benefici.

Misure di accountability.
Le misure di accountability più importanti introdotte dal regolamento UE sono: il **Registro dei trattamenti**, la designazione del **Data Privacy Officer** e la **Notifica dei Data Breach**.

Registro dei trattamenti ex art. 30 GDPR 679/2016.
Il Registro dei trattamenti costituisce una misura di accountability perché - essendo la fotografia dello stato di adeguamento privacy della struttura - fornisce al titolare la possibilità di documentare il proprio impegno nell'applicazione della nuova disciplina.
Le Linee Guida suggeriscono addirittura a tutti i Titolari l'adozione di questo Registro sebbene la legge Ue lo imponga soltanto alle imprese con non meno di 250 dipendenti o a quelle che trattano dati su larga scala come il settore bancario, assicurativo e dei trasporti.

Data Privacy Officer ex art. 37,38,39 GDPR 679/2016.
La designazione del Data Privacy Officer costituisce una misura di accountability fondamentale in quanto dimostra la volontà di adeguamento del Titolare che si appoggia a questa figura per tutti gli incombenti:

- Consultazione privacy questioni critiche;
- Formazione del personale;
- Valutazione di impatto dei trattamenti sui diritti degli interessati (PIA)
- Redazione della Privacy Governance;
- Redazione delle lettere di Incarico;
- Redazione dei Contratti Titolare-Responsabile;
- Relazioni con le Authority;
- Istruzioni sulla tenuta del Registro dei trattamenti.

Il Regolamento UE prevede l'**obbligo della designazione** del DPO per le autorità e gli organismi pubblici; per i Titolari che trattano dati su larga scala come settore bancario, assicurativo o dei trasporti; per i Titolari che trattano dati sensibili; per i Titolari che trattano dati giudiziari. Si ricordi inoltre che il DPO deve restare **indipendente** dal Titolare anche perché deve **sorvegliare** in modo oggettivo sull'esecuzione delle procedure di adeguamento privacy.

Notifica dei Data Breach ex art. 33 e 34 GDPR 679/2016.
La Notifica dei Data Breach entro 72 ore al Garante interno costituisce una misura di accountability in quanto consente al titolare di documentare la proprio volontà di applicazione della nuova disciplina privacy. L'art. 33 (5) GDPR 2016/679 dispone infatti che *"il titolare del trattamento **documenta qualsiasi violazione** dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'Autorità di controllo di verificare il rispetto del presente articolo".* Le Linee Guida suggeriscono ai Titolari di documentare in ogni caso le violazioni registrate anche se non notificate all'autorità di controllo né comunicate agli Interessati perché questa documentazione resta agli atti della struttura che potrà così provare in caso di accertamento la proprio buona condotta.

Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

TRASFERIMENTI DI DATI VERSO PAESI TERZI E ORGANISMI INTERNAZIONALI

(Artt. 44-50 GDPR 2016/679)

Comunicazione o trasferimento dei dati a Paesi extra UE e a Organizzazioni internazionali.

Il trattamento dei dati può consistere anche in una loro comunicazione all'Estero sia all'interno che all'esterno dell'Unione Europea nell'ambito di iniziative volte a favorire il processo di internazionalizzazione delle attività del titolare.

La comunicazione o il trasferimento dei dati verso Paesi terzi EXTRA UE o verso Organizzazioni internazionali avviene esclusivamente quando sussista almeno una delle seguenti condizioni:

- esiste una **decisione di adeguatezza** della Commissione UE pubblicata in Gazzetta UE;
- il Paese EXTRA UE o l'Organizzazione internazionale hanno dato **prova di avere adottato garanzie privacy adeguate** o opportune. Tale prova può essere fornita anche mediante l'adesione ad appositi **codici di condotta**;
- esistono **norme vincolanti di impresa**;
- esiste il **legittimo interesse del titolare** del trattamento.

Il Titolare si impegna a fornire **all'interessato** i mezzi per ottenere una **copia dei dati comunicati** all'estero o a favorire l'accesso al luogo materico o digitale dove sono stati resi disponibili.

Decisioni di adeguatezza.

La più importante **Decisione di adeguatezza** sinora adottata dalla **Commissione** è la **n. 2016/1250** del 12 luglio 2016 che ha riconosciuto all'**Accordo "EU-U.S. Privacy Shield"** un adeguato target di protezione dei dati trasferiti dall'Unione europea a Soggetti-Titolari con sede legale negli Stati Uniti "certificati" ai sensi del ridetto "Privacy Shields".

Esistono **altre Decisioni** di adeguatezza della Commissione UE nei confronti dei seguenti Paesi: Andorra, Argentina, Australia – PNR, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay.

Clausole Contrattuali Standard.

Si tratta di clausole contrattuali valutate dalla Commissione UE e ritenute adeguate. Pertanto incorporando il testo delle ridette clausole in un contratto utilizzato per il trasferimento, *"l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai principi stabiliti nella Direttiva anche nel Paese terzo di destinazione".* Si veda al seguente link:
http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1

BCR - Binding Corporate Rules.

Si tratta di clausole contrattuali utilizzate per il trasferimento dei dati verso Paesi extra UE tra società facenti parti dello stesso gruppo d'impresa.

"Si concretizzano in un documento contenente una serie di clausole (rules) che fissano i principi vincolanti (binding) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (corporate).

Le Bcr costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali" Si veda al seguente link: http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1