
NUOVO REGOLAMENTO UE SULLA PRIVACY

Linea Guida applicativa

Il Garante per la privacy ha elaborato una prima Guida all'applicazione del Regolamento UE 2016/679 in materia di protezione dei dati personali.

La Guida traccia un quadro generale delle principali innovazioni introdotte dalla normativa e fornisce indicazioni utili sulle prassi da seguire e gli adempimenti da attuare per dare corretta applicazione alla normativa, già in vigore dal 24 maggio 2016 e che sarà pienamente efficace dal 25 maggio 2018. L'obiettivo della Guida è duplice: da una parte offrire un primo "strumento" di ausilio ai soggetti pubblici e alle imprese che stanno affrontando il passaggio alla nuova normativa privacy; dall'altro far crescere la consapevolezza sulle garanzie rafforzate e sui nuovi importanti diritti che il Regolamento riconosce alle persone.

Il testo della Guida è articolato **in 6 sezioni** tematiche: fondamenti di liceità del trattamento; informativa; diritti degli interessati; titolare, responsabile, incaricato del trattamento; approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili; trasferimenti internazionali di dati.



Fondamenti di liceità del trattamento



Informativa



Diritti degli interessati (accesso, cancellazione-oblio, limitazione del trattamento, opposizione, portabilità)



Titolare, responsabile, incaricato del trattamento



Approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili (valutazione di impatto, registro dei trattamenti, misure di sicurezza, violazioni dei dati personali, nomina di un RDP-DP)



Trasferimenti internazionali di dati



1. 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** (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).

In particolare:

- **“Consenso”**

Cosa cambia: Per i dati "sensibili" (si veda art. 9 regolamento) il consenso **DEVE** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

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); inoltre, il titolare (art. 7.1) **DEVE** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Il **consenso dei minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

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 (*si veda considerando 46*)

- **“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.

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.



2. Informativa

- **“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. In particolare, il titolare **DEVE SEMPRE** specificare i **dati di contatto del RPD-DPO**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, 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.). 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 e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee (*si veda anche considerando 58*). L'informativa è data, **in linea di principio, per iscritto e 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*); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea. 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*), anche se 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.

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. In tutti i casi, il titolare deve specificare **la propria identità e 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**, e **quali sono i destinatari dei dati**.



3. Diritti degli interessati

Cosa cambia: Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili 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.

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. 12.5), 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).

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

- “Modalità per l’esercizio dei diritti”

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 (artt. 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).

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni (si veda il paragrafo "Cosa cambia"). 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).

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”**

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**.

- **“Diritto di cancellazione”**

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”**

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), bensì 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).

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”**

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) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"forniti" dall'interessato** al titolare (*si veda il considerando 68 per maggiori dettagli*).

Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.



4. Titolare, responsabile, incaricato del trattamento

Cosa cambia: disciplina la **contitolarità del trattamento** (*art. 26*) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

fissa più dettagliatamente (*rispetto all'art. 29 del Codice*) le **caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, 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 a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

consente la **nomina di sub-responsabili del trattamento** da parte di un responsabile (*si veda art. 28, paragrafo 4*), per specifiche attività di

trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo **risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (*si veda art. 82, paragrafo 1 e paragrafo 3*);

prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti (*ex art. 30, paragrafo 2*); l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti (*ex art. 32 regolamento*); la **designazione di un RPD-DPO**, nei casi previsti dal regolamento o dal diritto nazionale (*si veda art. 37 del regolamento*). Si ricorda, inoltre, che **anche il responsabile** non stabilito nell'Ue dovrà **designare un rappresentante** in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice.

Cosa non cambia: Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (*ex art. 30 Codice*), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (*si veda, in particolare, art. 4, n. 10, del regolamento*).



5. Approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili (valutazione di impatto, registro dei trattamenti, misure di sicurezza, violazioni dei dati personali, nomina di un RDP-DPO).

Cosa cambia: Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (*si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento*). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" (*si veda art. 25*), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (*si vedano considerando 75-77*); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (*si vedano artt. 35-36*) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia. Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.



5. Trasferimenti di dati verso paesi terzi e organismi internazionali

Cosa cambia: In primo luogo, **viene meno il requisito dell'autorizzazione nazionale** (*si vedano art. 45, paragrafo 1, e art. 46, paragrafo 2*). Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del regolamento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto attualmente previsto dall'art. 44 del Codice. Tuttavia, **l'autorizzazione del Garante sarà ancora necessaria** se un titolare desidera utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure **accordi amministrativi** stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.

Il regolamento consente di ricorrere anche a **codici di condotta ovvero a schemi di certificazione** per dimostrare le "garanzie adeguate" previste dall'art. 46. Ciò significa che i **titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta** o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. **Tuttavia** (*si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2*), tali titolari dovranno **assumere**, inoltre, **un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento** che sia giuridicamente vincolante e azionabile dagli interessati.

Il regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di **decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo**, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (*si veda art. 48*). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'art. 49. A tale riguardo, si deve ricordare che il regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un **interesse pubblico riconosciuto dal diritto dello Stato membro** del titolare o dal diritto dell'Ue (*si veda art. 49, paragrafo 4*) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

Il regolamento **fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme**. L'elenco indicato al riguardo nel paragrafo 2 dell'art. 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad

ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza di cui agli artt. 63-65 del regolamento – ossia, **è previsto in ogni caso l'intervento del Comitato europeo per la protezione dei dati** (si veda art. 65, paragrafo 1, lettera d)).

Cosa non cambia: Il regolamento (si veda Capo V) ha confermato l'approccio attualmente vigente in base alla direttiva 95/46 e al Codice italiano per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

i) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea (si veda art. 44, comma 1, lettera b), del Codice);

ii) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello) (si veda Art. 44, comma 1, lettera a) del Codice);

iii) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (corrispondenti in parte alle disposizioni dell'art. 43, comma 1, del Codice).

Le decisioni di adeguatezza sinora adottate dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica (si vedano art. 45, paragrafo 9, e art. 96). Restano valide, conseguentemente, le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione. Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi (si veda art. 46, paragrafo 5), sino a loro eventuale modifica (si veda la sezione "Cosa cambia" per maggiori dettagli
