giuricivile
RASSEGNA DI DIRITTO E GIURISPRUDENZA CIVILE

Il "Pacchetto Europeo Protezione Dati": le novità in materia di protezione del trattamento dei dati personali e della loro circolazione

di ***Paola Pagliarusco***

Parte III – Adempimenti per i Titolari del trattamento

Sommario: Premessa – **1.** Obblighi generali – **1.1** Titolare del trattamento, Responsabile del Trattamento e Responsabile della protezione dei dati personali (Data Protection Officer) – **1.2** Protezione dei dati "by design" e "by default" – **1.3** Registri delle attività di trattamento – **1.4** Cooperazione con l'autorità di controllo – **2.** Adempimenti a garanzia della sicurezza dei dati personali – **2.1** Misure di sicurezza – **2.2** Obbligo di notifica delle violazioni e comunicazione di una violazione dei dati personali all'interessato – **2.3** Valutazione di impatto e consultazione preventiva – **3.** Compliance aziendale: codici di condotta e certificazione – **3.1** Codici di condotta e monitoraggio – **3.2** Certificazione e organismi di certificazione – **4.** Trasferimenti di dati verso Paesi terzi o Organizzazioni internazionali – **4.1** Norme vincolanti d'impresa.

Premessa

Questo terzo contributo conclude l'analisi e l'approfondimento della normativa in materia di protezione e circolazione del dati, introdotta - come ormai noto - dal Regolamento UE 2016/679.

Dapprima, si è delineato il nuovo quadro normativo, istituzionale e sanzionatorio[1] posto dalla nuova disciplina; con il secondo contributo è stato approfondito l'aspetto delle nuove garanzie a tutela degli interessati[2]; infine, in questo terzo ed ultimo intervento, l'attenzione vien posta sui nuovi obblighi e/o adempimenti a carico dei Titolari e Responsabili del trattamento dei dati.

Il **25 maggio 2018** è una data che imprese, privati e pubbliche amministrazioni devono tenere bene a mente, in quanto **data ultima per conformarsi alle prescrizioni dato che il Regolamento diverrà pienamente efficacie**.

Va sottolineato che il Legislatore europeo, disponendo tale efficacia differita alla norma in commento, ha concesso ben due anni per consentire ai Titolari del trattamento (siano essi imprese, privati, pubbliche autorità o altri enti) di conformarsi alle prescrizioni.

La nuova disciplina, infatti, introduce una serie di adempimenti a carico della persona fisica o giuridica, dell'autorità pubblica o altro organismo, che abbia il potere di determinare le finalità e i mezzi del trattamento di dati personali altrui (il cd. "Titolare del trattamento")[3].

Volendo mantenere fede alle classificazioni del Regolamento, gli oneri che gravano su chi tratta dati personali possono essere suddivisi in quattro macro-aree:

1. **Obblighi generali** (Titolare del trattamento, Responsabile del Trattamento e Responsabile della protezione dei dati personali (Data Protection Officer); Protezione dei dati "by design" e "by default";

[1] Paola Pagliarusco, "Pacchetto protezione dati UE 2016: le novità in materia di protezione, circolazione e trattamento dei dati personali (parte I)", in Giuricivile, 2017, 4, (ISSN 2532-201X), http://giuricivile.it/pacchetto-protezione-dati-ue-2016-protezione-trattamento-dati-personali-della-circolazione/http://giuricivile.it/pacchetto-protezione-dati-ue-2016-protezione-trattamento-dati-personali-della-circolazione/

[2] Paola Pagliarusco, "Pacchetto protezione dati UE 2016: le novità in materia di protezione, circolazione e trattamento dei dati personali (parte II)", in Giuricivile, 2017, 4, (ISSN 2532-201X), http://giuricivile.it/pacchetto-protezione-dati-ue-parte-2/

[3] Vd. Definizione di Titolare del trattamento all' art. 4, n. 7. Regolamento UE 2016/679.

Registri delle attività di trattamento; Cooperazione con l'autorità di controllo);

2. Adempimenti a garanzia della sicurezza dei dati personali (Misure di sicurezza; Obbligo di notifica delle violazioni e comunicazione di una violazione dei dati personali all'interessato; Valutazione di impatto e consultazione preventiva);

3. Compliance aziendale: codici di condotta e certificazione (Codici di condotta e monitoraggio; Certificazione e organismi di certificazione);

4. Trasferimenti di dati verso Paesi terzi o Organizzazioni internazionali (Norme vincolanti d'impresa)

1. Obblighi generali

Il Regolamento prevede un aumento della responsabilità a carico del Titolare, la creazione di meccanismi di tracciabilità che consentano di allocare all'interno delle aziende le responsabilità per il trattamento dei dati personali e, soprattutto, la gestione dei dati diventa un vero e proprio processo aziendale da gestire e del quale occorre tener conto nell'organizzazione dell'impresa.

Ma vediamo più da vicino come si esplica tutto ciò.

1.1 Titolare del trattamento, Responsabile del Trattamento e Responsabile della Protezione dei Dati personali (Data Protection Officer)

Alle figure di riferimento in materia di Protezione dei dati - il Titolare del Trattamento e il Responsabile del Trattamento – si aggiunge, ora, il Responsabile (o Rappresentante) della protezione dei dati[4].

Il Regolamento fornisce le definizioni di questi tre soggetti (art. 4 nn. 7, 8 e 17):

- **Titolare del trattamento**: "***la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali****; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*";

- **Responsabile del trattamento**: "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che* ***tratta dati personali per conto del titolare del trattamento***";

- **Rappresentante** (anche detto DPO): "*la persona fisica o giuridica* ***stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto*** *ai sensi dell'articolo 27,* ***li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento***".

Il DPO rappresenta una novità assoluta e rappresenta la figura professionale incaricata di svolgere un'attività di controllo e supporto strategico-organizzativo circa le decisioni operative del Titolare del trattamento, affinché venga rispettata la normativa di riferimento.

Tale figura è destinata ad avere un forte impatto nell'organizzazione di Enti sia pubblici[5], sia privati.

Infatti, l'obbligo grava sui Titolari e Responsabili del trattamento "*le cui attività principali consistono in* ***trattamenti che richiedono un***

[4] RPD, ovvero DPO se si utilizza l'acronimo inglese c.d. Data Protection Officer.
[5] "eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali", cfr. Cons. (97, GDPR).

monitoraggio regolare e sistematico degli interessati su larga scala, o *ove le attività principali del titolare del trattamento o del responsabile del trattamento* ***consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati***"[6].

Il Considerando (97) chiarisce la *ratio* sottesa all'introduzione del DPO: fornire al Titolare (o Responsabile del trattamento) l'assistenza di un professionista con specifiche competenze tecnico-giuridiche in materia di protezione dei dati.

Solitamente, infatti, specie nel settore privato, il Titolare del trattamento è impegnato a svolgere le sue attività primarie afferenti il *business*, e l'attività di trattamento dei dati finisce per essere solo accessoria e ciò comporta una scarsa attenzione e un basso livello si sicurezza nel trattamento dei dati.

Per ovviare a questa prassi, la normativa UE prevede l'obbligo di dotarsi della figura del DPO/RPD il quale può essere un libero professionista o un dipendente, ma in ogni caso ha il dovere di compiere le proprie funzioni in modo indipendente, considerando i rischi in relazione al contesto specifico del singolo trattamento.

Alla luce del combinato disposto degli artt. 37, par. 5 e 39, il DPO deve essere designato sulla base di specifiche competenze professionali, "*in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati*", nonché della capacità di assolvere i compiti che gli sono affidati e che così si possono riassumere:

1. informare e fornire consulenza in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

2. sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

[6] Cfr. Considerando (97) e art. 37, par. 1, Regolamento UE 2016/679 (c.d. GDPR).

3. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

4. cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Per rendere possibile tutto ciò, sono previsti specifici obblighi in capo al Titolare e Responsabile del trattamento:

1. assicurare un flusso informativo tempestivo e adeguato per tutte le questioni relative alla protezione dei dati;

2. sostenere il DPO nell'esecuzione dei suoi compiti fornendogli le risorse necessarie e assicurandosi che egli non riceva istruzioni da alcun soggetto;

3. assicurare che eventuali altri compiti svolti dal DPO non siano in conflitto di interessi con il ruolo di Responsabile della protezione.

Va sottolineato che tale Organo è tenuto al segreto rispetto all'adempimento delle proprie funzioni e può essere interpellato da qualsiasi interessato voglia avere notizie circa il trattamento dei propri dati e dei relativi diritti derivanti dal Regolamento.

1.2 Approccio basato sul rischio e misure di *accountability* di Titolari e Responsabili del trattamento: Protezione dei dati "*by design*" e "*by default*" (art. 25)

Il considerando (78) prevede che la tutela dei diritti e delle libertà degli interessati passi attraverso la necessaria adozione di misure tecniche e organizzative tali da garantire la protezione dei dati fin dalla progettazione (*Privacy by design*) e per impostazione predefinita (*Privacy by default*).

Per rendere effettiva la sicurezza dei trattamenti, dunque, i Titolari del trattamento dovranno adottare politiche interne e attuare misure che si

basino su una progettazione che tenga conto *ab initio* della protezione dei dati e che si traduca, necessariamente, in una tutela dei dati "*di default*".

Considerando le condizioni e peculiarità del singolo caso, il Titolare del trattamento dovrà attivarsi per progettare un processo aziendale e gli opportuni applicativi informatici di supporto per garantire che vengano trattati "*di default*" solamente i dati personali necessari per ogni specifica finalità di trattamento.

Si badi che un meccanismo di certificazione approvato ai sensi del Regolamento, come si vedrà[7], può fungere da elemento atto a dimostrare la conformità ai requisiti di "*Privacy by design*" e "*Privacy by default*" richiesti dalla GDPR.

Dalla Guida all'applicazione del Garante della Privacy[8], emanata con comunicato stampa dello scorso 28 Aprile 2017, si evince come il Regolamento abbia posto l'accento sulla "responsabilizzazione"[9] di Titolari e Responsabili, affinché adottino dei comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

Infatti, ai Titolari del trattamento viene chiesto di adoperarsi autonomamente alla progettazione di processi e di misure rispondenti alla normativa europea, pur nel rispetto di alcuni criteri specifici indicati nel regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "***data protection by default and by design***", ossia la 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.

[7] Cfr. paragrafo i
[8] Cfr. http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali
[9] Accountability nell'accezione inglese.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio: il Legislatore richiede venga eseguita un'analisi preventiva da parte dei Titolari che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

Dice la Guida del Garante che fra tali attività sono indispensabili quelle connesse al secondo criterio_individuato nel Regolamento, ossia il **rischio inerente al trattamento**.

Esso deve essere preventivamente valutato, come vedremo al successivo par. g., attraverso un'apposita Valutazione d'impatto sulla protezione dei dati e consultazione preventiva (artt. 35 e ss.).

All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento ovvero consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale.

In questa nuova cornice, ove le verifiche dell'Autorità di controllo saranno necessariamente *ex post*, alcuni istituti previgenti, come la notifica preventiva dei trattamenti all'Autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare: si veda art. 17 Codice), lasceranno il posto a nuovi obblighi, quali la tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, l'effettuazione di valutazioni di impatto in piena autonomia (cfr. par. a. e g.)

1.3 Registro delle attività di trattamenti

È sicuramente tra le novità più interessanti del Regolamento, anche se dal sapore di "déjà-vu": impossibile, infatti, non pensare al Documento Programmatico per la Sicurezza dei dati (DPS) previsto dal nostro Codice Privacy che è stato per quasi dieci anni il principale adempimento per le aziende in materia di protezione dei dati e con il quale presenta alcune analogie.

Il Regolamento si occupa del Registro delle Attività di Trattamento, così motivandone l'introduzione al Considerando 82: necessaria presenza, presso ogni Titolare del trattamento, di un documento ove rendicontare tutte le attività in materia di protezione e circolazione dei dati al fine di dimostrare la conformità alle disposizioni di legge.

Nel corpo del Regolamento, all'art. 30, si trova, invece, la precisa descrizione dell'istituto, con l'elencazione dei contenuti richiesti.

Vengono previsti due diversi Registri delle attività:

- il **paragrafo 1** detta le informazioni contenute dal Registro che deve essere tenuto dal Titolare del Trattamento e, ove applicabile, dal suo Rappresentante, relativamente alle attività svolte sotto la propria responsabilità;

- il **paragrafo 2**, invece, detta le informazioni che deve contenere il Registro tenuto da ogni Responsabile del trattamento e, ove applicabile, dal suo Rappresentante, relativamente a tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento.

Entrambi i registri sono tenuti in forma scritta, anche in formato elettronico e, se richiesto, devono essere messi a disposizione dell'Autorità di controllo.

Importante precisazione fatta dal Legislatore europeo è che **l'obbligo del Registro non si applica alle imprese od organizzazioni con meno di 250 dipendenti**, ad eccezione dei casi in cui il trattamento:

1. possa presentare un rischio per i diritti e le libertà dell'interessato;

2. non sia occasionale;

3. riguardi categorie particolari di dati personali o dati personali relativi a condanne penali e a reati.

Nella Guida del Garante si legge che il Registro rappresenterà uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte dell'Autorità di controllo, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio.

1.4 Cooperazione con l'autorità di controllo (art. 31);

Nel novero degli adempimenti di portata generale, il Regolamento espressamente pone a carico del Titolare e del Responsabile del trattamento uno specifico obbligo di cooperazione con l'Autorità di controllo; in quest'ottica rientra anche la necessaria esibizione, su richiesta, dei registri delle attività di trattamento, di cui al punto precedente.

2. Adempimenti a garanzia della sicurezza dei dati personali

2.1 Misure di sicurezza (art. 32)

Allo scopo di mantenere la sicurezza e prevenire trattamenti in violazione al Regolamento, il Titolare e il Responsabile devono porre in essere misure tecniche ed organizzative tali da "*garantire un livello di sicurezza adeguato al rischio*" del trattamento (art. 32, paragrafo 1); in questo senso, specifica la Guida del Garante[10], la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva.

Dopo il 25 maggio 2018 cesseranno di sussistere gli obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al Titolare e al Responsabile in rapporto ai rischi specificamente individuati come da art. 32.

[10] http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

Preme sottolineare anche la possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate (vd. par. h. e i.).

2.2 Notifica delle violazioni di dati personali all'autorità di controllo (art. 33) e comunicazione di una violazione dei dati personali all'interessato (art. 34)

Con l'effettiva applicazione del Regolamento, sul Titolare grava anche l'obbligo di documentare qualsiasi violazione dei dati personali e di notificarle all'Autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza (art. 33).

Del pari, qualora la violazione rappresenti un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare ha, altresì, l'obbligo di darne comunicazione all'interessato con linguaggio semplice e chiaro.

Detta comunicazione non è richiesta se è soddisfatta almeno una delle seguenti condizioni:

a) Il Titolare ha messo in atto misure tecniche e organizzative adeguate di protezione, applicate ai dati oggetto della violazione;

b) Il Titolare ha successivamente adottato misure volte a scongiurare un possibile rischio elevato per i diritti e le libertà delle persone fisiche;

c) La comunicazione richiederebbe sforzi sproporzionati.

Il legislatore detta con precisione sia i contenuti della notifica (par. 3, art. 33) sia della comunicazione (par. 2, art. 34).

2.3 Valutazione di impatto sulla protezione dei dati e consultazione preventiva (artt. 35-36)

Come anticipato sommariamente al paragrafo b., la valutazione d'impatto è l'attività preventiva che deve essere effettuata dal Titolare per ottemperare al requisito richiesto da Regolamento circa il rischio inerente al trattamento.

Secondo quanto esposto dallo stesso Legislatore al Considerando (84), la valutazione di impatto mira a potenziare il rispetto della GDPR attraverso la determinazione dell'origine, la natura, la particolarità e la gravità del rischio a cui il trattamento dei dati potrebbe sottoporre i diritti e le libertà delle persone fisiche.

Infatti, qualora un trattamento, considerate le caratteristiche del caso specifico, preveda l'uso di nuove tecnologie e rappresenti un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare, prima di procedere al trattamento, dovrà svolgere una **valutazione dell'impatto** che tale trattamento avrà sulla protezione dei dati personali.

La suddetta Valutazione è richiesta, ai sensi dell'art. 35, par. 3, nei seguenti casi:

1. Valutazione globale di aspetti personali, basata sul trattamento automatico, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici i incidono significativamente sulle persone fisiche;

2. Trattamento su vasta scale di dati personali sensibili o dati relativi a condanne penali e a reati;

3. Sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Peraltro, si prevede che l'Autorità di controllo rediga e renda pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto; diversamente, detta Autorità ha la facoltà (e non il dovere) di redigere un elenco analogo ove rendere noti quei trattamenti che non necessitano della Valutazione *de quo* (par. 4 e 5).

Il contenuto della Valutazione viene descritto al paragrafo 7 nel suo contenuto minimo necessario ("*almeno*"); il Legislatore ribadisce che, anche in questo caso, terrà in debito conto il rispetto di appositi codici di condotta approvati conformemente al Regolamento.

Qualora la suddetta Valutazione d'impatto evidenzi che il trattamento potrebbe rappresentare un rischio elevato in assenza dell'applicazione delle misure adottate dal Titolare, quest'ultimo ha il dovere di consultare preventivamente l'Autorità di controllo (art. 36), la quale fornirà un parere scritto al Titolare o al Responsabile (ove nominato) entro 8 settimane dal ricevimento della richiesta di consultazione.

3. Compliance aziendale: codici di condotta e certificazione

Con la Sezione 5 del Regolamento - rubricata "*Codici di condotta e Certificazione*" – il Legislatore europeo esprime il proprio favore per le procedure di certificazione, incoraggiandone l'utilizzo da parte degli Enti tramite il riconoscimento ufficiale di tali strumenti di compliance quale prova di ottemperanza alla normativa in esame.

Tali strumenti sono i codici di condotta e le procedure di certificazione.

3.1 Codici di condotta e monitoraggio.

Il Regolamento "incoraggia" l'elaborazione di codici di condotta al fine di "*facilitarne l'effettiva applicazione, tendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese*"[11].

La normativa europea definisce l'*iter* di approvazione di questi codici di condotta.

[11] Considerando (98), Regolamento 2016/679.

Le associazioni di categoria e gli altri organismi rappresentanti le categorie di Titolari, possono elaborare dei codici di condotta sottoponendo il progetto di codice (ovvero la modifica o la proroga) all'Autorità di controllo competente, la quale esprimerà un parere sulla conformità al Regolamento e, se lo riterrà idoneo, approverà il codice, lo registrerà e lo pubblicherà.

Qualora il progetto di codice di condotta riguardi attività di trattamento in vari Stati membri, prima di approvarlo, l'Autorità competente lo sottopone all'esame del Comitato (tramite il meccanismo di coerenza di cui all'art. 63) il quale formula un parere sulla conformità al Regolamento del progetto o sulla previsione di sufficienti garanzie e, in caso di parere positivo, trasmette il progetto alla Commissione.

Quest'ultima potrà decidere, mediante atti di esecuzione, che il codice di condotta abbia valenza generale all'interno dell'Unione.

In tal caso, la Commissione provvede a darne adeguata pubblicità e diffusione.

Il Comitato raccoglie in un registro tutti i codici di condotta e li rende pubblici.

Il **monitoraggio** sulla conformità dei suddetti codici viene delegato ad organismi in possesso di un adeguato livello di competenze e dell'accreditamento dell'Autorità di controllo competente, accreditamento che può essere revocato se l'organismo non ha o non ha più i requisiti richiesti.

Tali organismi hanno il potere di adottare le opportune misure in caso di violazione del codice da parte del Titolare (o del Responsabile) del trattamento, informando l'Autorità di controllo competente.

Detto monitoraggio, previsto all'art. 41, non si applica ai trattamenti effettuati da autorità pubbliche o da organismi pubblici.

3.2 Certificazione e organismi di certificazione

Come per i codici di condotta pocanzi trattati, la nuova normativa europea recita:

"*Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere* ***incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi***"[12].

I meccanismi, i sigilli e i marchi approvati secondo il paragrafo 5 dell'art. 42 si possono estendere anche ai Titolari o Responsabili del trattamento non soggetti al DPGP, i quali, tuttavia, assumono l'impegno vincolante al rispetto delle disposizioni normative in commento, mediante strumenti contrattuali o comunque giuridicamente vincolanti.

Anche in tale operazione sono tenute in debito conto le esigenze specifiche delle micro, piccole e medie imprese.

La certificazione deve essere volontaria e accessibile tramite una procedura trasparente, viene rilasciata dall'Autorità di controllo competente o da organismi di certificazione dotati dell'adeguato livello di competenze riguardo alla protezione dei dati che devono essere accreditati da uno, o da entrambi, dei seguenti organismi:

1. Autorità di controllo competente;
2. Organismo nazionale di accreditamento designato secondo la normativa europea conformemente alla norma orma ISO/IEC 17065:2012 per l'accreditamento degli Organismi di certificazione di prodotti, processi e sevizi[13].

La certificazione viene rilasciata per un massimo di tre anni, trascorsi i quali deve necessariamente essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti, altrimenti essa viene revocata.

[12] Considerando (100), Regolamento 2016/679.
[13] La norma contiene requisiti per la competenza, il funzionamento coerente e l'imparzialità degli organismi di certificazione di prodotti, processi e servizi.

Il Comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e si occupa di renderli pubblici con i mezzi adeguati.

4. Trasferimenti di dati verso Paesi terzi o Organizzazioni internazionali

Il Titolare (o il Responsabile) del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo a seguito della decisione della Commissione ovvero, in mancanza di questa, solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi (artt. 45-46).

Oltre ai mezzi previsti ed enucleati dal Regolamento al paragrafo 2 dell'art. 46, il Legislatore europeo prevede anche la possibilità di prevedere dei "pacchetti" di norme applicabili uniformemente ai gruppi di imprese, volti a regolamentare il trasferimento transfrontaliero di dati.

4.1 Norme vincolanti d'impresa (art. 47)

La *ratio* consiste nel fatto che "*un gruppo imprenditoriale o un gruppo di imprese che svolge un'attività economica comune dovrebbe poter applicare le norme vincolanti d'impresa approvate per i trasferimenti internazionali dall'Unione agli organismi dello stesso gruppo imprenditoriale o gruppo d'imprese che svolge un'attività economica comune, purché tali norme contemplino tutti i principi fondamentali e diritti azionabili che costituiscano adeguate garanzie per i trasferimenti o categorie di trasferimenti di dati personali*"[14].

Anche dette "BCR", consistono in una serie di clausole contrattuali che dettano principi (in linea con il Regolamento 679/2016 e che assicurano un

[14] Cfr. Considerando (110), Regolamento 2016/679

livello di protezione adeguato) vincolanti per tutte le società facenti parte del gruppo[15].

Si tratta nello specifico di norme approvate dall'Autorità di controllo, secondo il meccanismo di coerenza e purché rispettino le seguenti condizioni:

1. Siano giuridicamente vincolanti per tutti i membri del gruppo imprenditoriale o di imprese che svolgono attività economica comune;
2. Conferiscano agli interessati diritti azionabili;
3. Soddisfino i requisiti minimi previsti dal Regolamento.

[15] Avv. Cristiano Cominotto – Avv. Anna Minichiello – Dott. Francesco Curtarelli, "Il trasferimento dei dati personali in Paesi extra UE", in Diritto24 alla pag. http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2016-10-03/il-trasferimento-dati-personali-paesi-extra-ue-180336.php?preview=true