DirICTo
Diritto & Information and Communication Technology

ICT4Law & Forensics

PRIVACY E CLOUD ALLA LUCE DEL NUOVO REGOLAMENTO UE

smau
MILANO 24-26 OTTOBRE 2017
fieramilanocity

Massimo Farina

www.massimofarina.it
massimo@massimofarina.it
www.diricto.it/

Chi siamo

DirICTo

Diritto & Information and Communication Technology

DirICTo è un network che raggruppa esperti e studiosi, di tutta l'Italia, in materia di Diritto dell'Informatica e dell'Informatica Giuridica con il fine di sviluppare attività di studio, ricerca e approfondimento nell'ambito delle tematiche di interesse comune per il mondo giuridico e informatico

Web site: **www.diricto.it**

Chi siamo

ICT4Law & Forensics

ICT for Law and Forensics è il laboratorio di Informatica Forense del Dipartimento di Ingegneria Elettrica e Elettronica dell'Università di Cagliari.

Aree di interesse: e-commerce e contrattazione telematica, la tutela giuridica dei domain names, privacy e protezione dei dati personali nel mondo telematico, cyber crimes, digital forensics

Web site: **ict4forensics.diee.unica.it**

PARTIAMO DA QUI

5 maggio 2016

Pubblicazione nella Gazzetta Ufficiale dell'Unione Europea il **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio, del 27 aprile 2016 , relativo alla «***protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE***».

SCOPO DEL REGOLAMENTO

offrire una **disciplina uniforme** per tutto il territorio UE, al fine di assicurare un elevato livello di protezione ed eliminare gli ostacoli inerenti la circolazione dei dati personali in ambito comunitario

DEADLINE PER L'ADEGUAMENTO

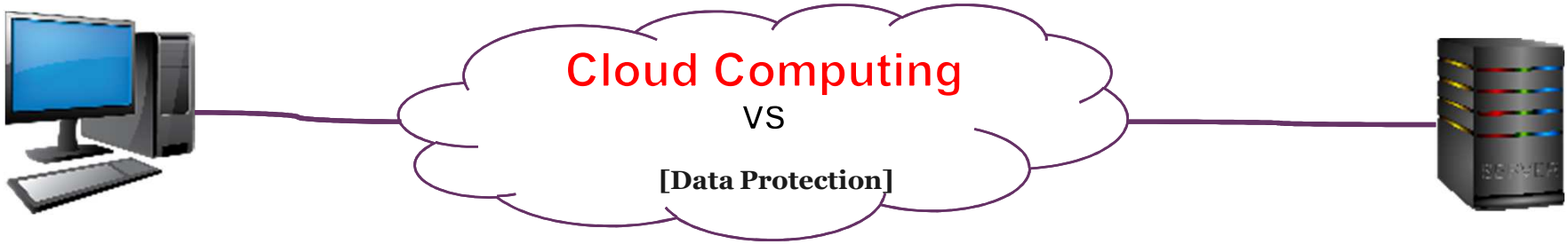
25 maggio 2018

Privacy vs Cloud

le imprese e le P.A. fanno uso sempre più frequente di piattaforme di ***Cloud Computing***

Perché il cloud?

elevata scalabilità, rapidità di accesso all'infrastruttura, ampia disponibilità, affidabilità e velocità



sistemi che memorizzano ed elaborano risorse di dati, attraverso la connettività di rete e il collegamento di server esterni, gestiti dal ***cd. "Cloud provider"***

L'approccio……sbagliato

Spesso quando si affronta il **rapporto tra Cloud Computing e protezione di dati personali**, si cercano regole specifiche e appositamente dedicate alla preservazione dei dati nei casi di *storage* in *cloud*

In realtà

le regole di **tutela dei dati personali** trattati **«in cloud»** seguono la disciplina generale e attribuiscono le medesime responsabilità dei trattamenti eseguiti con stesse linee generali di preservazione delle informazioni personali.

Adempimenti (prima e dopo)

ADEMPIMENTO	D.LGS 196/03	REG. UE 679/2016
NOTIFICA DEI TRATTAMENTI	SI	NO
DATA BREACH	NO	SI
INFORMATIVA	SI	SI
CONSENSO	SI	SI
REGISTRO DEI TRATTAMENTI	NO	SI
CODICE DI CONDOTTA	NO	SI
VALUTAZIONI DI IMPATTO	SI	SI
DATA PROTECTION BY DESIGN BY DEFAULT	NO	SI
DPO	NO	SI

I soggetti del Cloud

Fornitore del servizio
(cloud provider)

Utilizzatore del sistema Cloud
(l'impresa che si avvale del servizio)

Fruitore del servizio
(utente finale)

PRIMO PROBLEMA

potrebbe risultare non agevole inquadrare correttamente i ruoli dei soggetti coinvolti nella filiera:
"Titolare" e "Responsabile del trattamento"
e quindi le responsabilità.

Inquadramento soggettivo problematico

Quali ruoli e responsabilità in tema di protezione dei dati personali?

Utilizzatore del Cloud

Cloud Provider

fruitore del Cloud

Considerazioni preliminari

SE

alla luce delle definizioni presenti nel Reg. UE 679/2016

Utente del Cloud

=

Titolare del trattamento

Cloud Provider

=

Responsabile esterno del trattamento

ALLORA

Il titolare del trattamento deve costantemente accertare l'affidabilità e la competenza del responsabile esterno, oltre che adempiere agli obblighi organizzativi e gestionali di implementazione e controllo delle misure di sicurezza (che nel caso di specie sono di effettiva competenza del *provider*)

Considerazioni preliminari

MA

il rapporto sostanziale tra le parti spesso si presenta con connotati sostanziali differenti, rispetto a quelli preconfezionati dal legislatore

INFATTI

- La gran parte dei contratti stipulati per la fornitura di servizi di *cloud* **standardizzati** contengono clausole generali accettate, per adesione, dal cliente;

- di fatto, quindi, il *cloud provider* si colloca in una **posizione dominante** rispetto al fruitore del servizio, il quale non è nelle condizioni di poter negoziare le clausole a lui meno favorevoli.

Quindi ……nei contratti di cloud

La sostanza del rapporto vede entrambi i soggetti conservare una piena libertà decisionale in merito alle modalità del trattamento

- ogni **decisione relativa alle misure di sicurezza** da adottare e la **configurazione tecnologica** dei sistemi è di esclusiva **competenza del *provider***.

- il **Cliente**, benché sia titolare del trattamento, può **verificare l'esatta esecuzione delle prestazioni** in conformità con quanto previsto dal contratto, ma non può esercitare alcun potere di controllo sugli aspetti suddetti

VANNO RIVISTI I RUOLI PRECONFEZIONATI

Contitolarità?

Il fornitore del servizio non deve partecipare alla **definizione delle finalità di trattamento**.

Ammettere ciò, significherebbe licenziare **un'ingerenza** che non appartiene (e non deve appartenere) ai rapporti quivi contemplati, in particolare se il settore d'interesse riguarda titolari ai quali compete il trattamento di dati sensibili.

non vi sarebbe stato alcun dubbio sull'applicabilità di tale disposizione al rapporto tra *cloud provider* e cliente se il **ruolo del contitolare fosse stato circoscritto alla determinazione congiunta dei mezzi del trattamento**, e non anche delle finalità

Quindi ……nei contratti di cloud

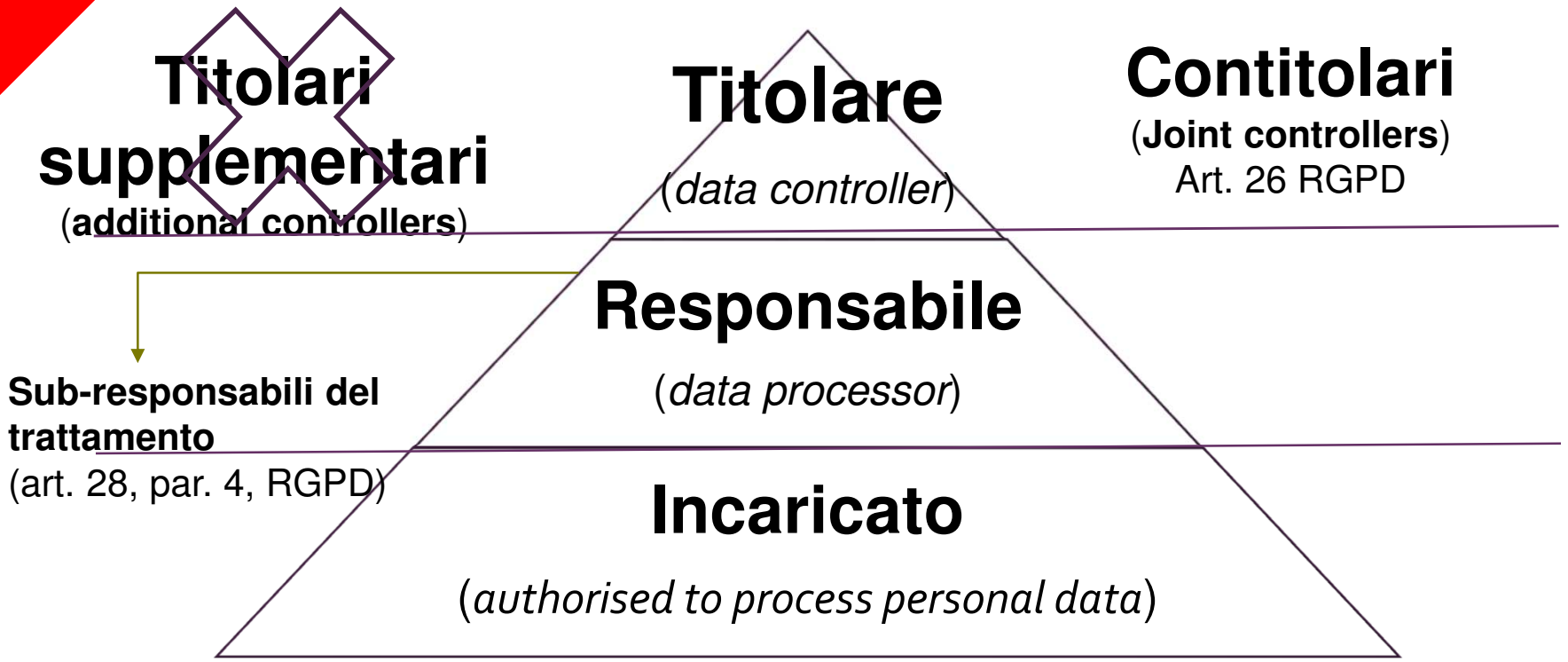
Il ruolo più appropriato per il *cloud provider* rimane quello della "**titolarità supplementare**"

questa non è stata la scelta del legislatore europeo

già contemplata per i **fornitori di servizi di telecomunicazioni**, ove il fornitore del servizio ha una titolarità limitata al "**funzionamento del servizio**".
(Direttiva 95/46/CE, considerando n. 47)

la contitolarità è presente nel momento in cui "*più titolari del trattamento* ***determinano congiuntamente le finalità e i mezzi del trattamento***

Ricapitolando



Il contratto di cloud computing

La necessità di qualificare il contratto di cloud computing si ripresenta per ogni specifica forma di servizio

LE RICOSTRUZIONI PIU' NOTE:

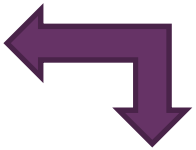
- L'appalto di servizi e la licenza d'uso
- La "locazione" di spazio *web*
- *L'outsourcing*

ma è anche possibile

partire dalla centralità dei dati come elemento di classificazione

Un possibile inquadramento contrattuale

La tipologia di *cloud* considerata in questa sede consiste principalmente nella gestione della circolazione dei **beni digitali** (documenti) per conto dell'ente pubblico o privato che si rivolge al *cloud provider*



il contratto consiste nell'affidare, al fornitore del servizio, i beni digitali da custodire mediante deposito

In base all'art. 1766 c.c. "*Il deposito è il contratto con il quale una parte* (depositario) *riceve dall'altra* (depositante) *una cosa mobile con l'obbligo di custodirla e restituirla in natura*"

Le prime due questioni da affrontare

1 i dati digitali possono essere annoverati tra i beni mobili di cui all'art. 812, comma 3, c.c.?

2 I dati digitali hanno natura fungibile o infungibile?

il **deposito regolare** ha per oggetto una cosa **infungibile** (la cosa deve essere conservata, custodita e **restituita in natura**);

Il **deposito irregolare** (art.,1782) ha per oggetto beni **fungibile** (p.e. il denaro), con facoltà del depositario di servirsi della cosa (di cui acquista la proprietà) e con l'obbligo, di restituirne altrettante della **stessa specie e qualità**.

I documenti sono beni?

I beni dell'informazione sembrano essere conformi alla definizione residuale di bene mobile contenuta nel codice civile

ma

Voci autorevoli escludono che oggetto del deposito possano essere beni immateriali

però

La stessa dottrina precisa che possono essere oggetto di deposito i beni che siano suscettibili di immagazzinamento e conservazione.

Nel tentativo di trovare concordanza tra tutte le posizioni, si potrebbe affermare che i beni digitali dell'informazione (i dati) sono, al contrario, idonei al deposito

Deposito regolare o irregolare ?

il bene digitale dell'informazione **è fungibile**, infatti, nel momento in cui viene restituito, **non è mai identico a quello depositato**

Ciò vale dal punto di vista strettamente tecnico-informatico, in quanto i dati elaborati (cioè letti da varie posizioni/applicazioni e trasmessi da diverse reti telematiche) **mutano continuamente** anche se rimangono **equivalenti nel loro significato intelligibile all'uomo.**

In conseguenza di ciò, i beni digitali depositati nella nuvola si presentano con **caratteristiche di fungibilità** e quindi oggetto di **deposito irregolare**

Deposito regolare o irregolare ?

Il cloud provider, depositario dei beni digitali dell'informazione, **non può servirsi, né diventare proprietario, dei dati che custodisce** e che appartengono al depositante.

Chi eroga il servizio di cloud ha precisi obblighi di riservatezza sugli stessi (ancor più se si tratta di dati sensibili), che provengono direttamente dalla legge, ancora prima che dal regolamento negoziale

Ciò accomuna il contratto di cloud computing al **deposito regolare**.

Il compromesso

Il deposito cloud, se di deposito si tratta, è di natura sui generis, quindi atipico, che **segue principalmente la disciplina del deposito regolare, fino a sconfinare**, seppure per risibili aspetti, **nel deposito irregolare**.

IRREGOLARE

Il depositario in cloud, che si riserva la facoltà di modificare la ubicazione, spostare, archiviare in vario modo i dati **ha l'obbligo di restituire**, quando richiesto, **beni digitali della stessa natura e specie ricomponendo gli archivi**.

REGOLARE

Il depositante conserva la titolarità dei propri dati, che, nonostante siano archiviati sulle memorie del depositario, non divengono mai di proprietà di quest'ultimo

N.B.: la titolarità sul dato non significa necessariamente proprietà ma anche semplicemente possesso, così da rendere (relativamente a quest'aspetto) il contratto di cloud pienamente compatibile con il contratto di deposito

Disciplina (generalità)

In base alle disposizioni codicistiche, il depositario deve:

- custodire la cosa;
- usare nella custodia la diligenza del buon padre di famiglia;
- non servirsi della cosa depositata;
- non dare la cosa depositata ad altri;
- restituirla a richiesta o al termine convenuto;
- restituire i frutti della cosa che egli abbia percepiti.

Da tali obbligazioni discende che la **responsabilità contrattuale del depositario** (e quindi anche quella del *cloud provider*) verte su tre principali aspetti:
custodia, diligenza e conservazione della cosa

Disciplina (onerosità)

In base alle disposizioni codicistiche,
il **deposito si presume a titolo gratuito**
(salvo diverso accordo tra le parti)

Non si può certamente pensare che il contratto di *cloud* possa affermarsi, e quindi diffondersi, nel mercato **a titolo gratuito**, visto che la qualità e la sicurezza, che ne sono alla base, comportano **investimenti notevoli per chi si impegna ad assicurarle**..

Disciplina (interoperabilità)

Tra gli obblighi del fornitore, va certamente prevista nel contratto di cloud la **garanzia di interoperabilità**, così da soddisfare **l'obbligo di restituzione tipico dei contratti di deposito**.

Si pensi, ad esempio, **all'impossibilità di ispezionare i dati** alloggiati sulla "nuvola", senza il consenso del depositario, che si traduce in una **forte limitazione** del diritto d'accesso.

Si pensi, altresì, al pericolo di **mancata restituzione futura** dei beni depositati, che si configurerebbe nel caso di restituzione di dati "illeggibili" (per via della detenzione in formato non interoperabile).

L'**interoperabilità**, al di la del suo risvolto pratico, **garantisce** il diritto del titolare dell'informazione digitale a conseguire l'**accesso** ai beni custoditi in una infrastruttura informatica attrezzata.

Libertà contrattuale e integrazione negoziale

CLAUSOLE CONTRATTUALI CONSIGLIATE

Divieto di cessione

Localizzazione dei Server

Divieto di subappalto

Legge applicabile

Foro Competente

Misure di sicurezza (risoluzione e penali per il mancato adeguamento)

Lock-in e way out (garanzia d'uscita e di distruzione del dato)

Libertà contrattuale e integrazione negoziale

CERTIFICAZIONI

- l'articolo 42 del Reg. UE 679/2016 incoraggia l'istituzione di meccanismi di **certificazione** della protezione dei dati per **dimostrare** che i trattamenti effettuati dai titolari e dai responsabili dei trattamenti siano conformi al Regolamento;
- le certificazioni si rilasciano in base a criteri **standard predefiniti**, che possono essere approvati solo dal Garante privacy e/o dal Comitato Europeo

MISURE DI SICUREZZA
(nuovo approccio)

DATA PROTECTION BY DESIGN AND BY DEFAULT

Il fornitore del servizio cloud con cui gli utilizzatori tratteranno i dati deve preoccuparsi di **costruire o ideare** lo un servizio dotato di **misure tecniche che garantiscano la sicurezza**, **disponibilità e integrità dei dati nonché il rispetto dei principi di protezione dei dati**.

La certificazione

Ancora nessuna certificazione

Ad oggi, non sono stati definiti i criteri e alcuni requisiti per l'accreditamento degli organismi di certificazione, e neppure i criteri per la certificazione.

Su questo, il Garante sta lavorando insieme alle altre Autorità dei Paesi Ue per definire, entro l'anno, un quadro comune di criteri per accreditare gli organismi di certificazione e per la certificazione.

ma

Nel contempo, è però già disponibile lo standard ISO/IEC 27018, elaborato nel 2014 da ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission)

lo standard ISO/IEC 27018

E' il primo standard a livello internazionale che contribuisce a garantire il rispetto dei principi e norme in materia di privacy, da parte dei provider di public cloud.

però

Si tratta di Linee Guida**, riferite al Sistema di gestione dell'Organizzazione**, accreditabili in base alla norma ISO/IEC 17021 (la precisazione è importante, perché si ricorda che invece **il Reg. privacy si riferisce a certificazioni di prodotto / servizio accreditabili in base alla norma ISO/IEC 17065**) che prendono in considerazione i requisiti normativi per la protezione dei dati personali per definire i possibili rischi per la sicurezza informatica di un fornitore di servizi cloud.

LO STANDARD 27018 Non è quindi una norma certificabile se presa come riferimento unico, ma è possibile ottenere una **integrazione del proprio certificato ISO/IEC 27001**, rilasciato da un Ente di certificazione accreditato, per dimostrare la capacità del provider di assicurare la protezione dei dati personali

Aspetti principali dello standard ISO 27018 (1/2)

- l'interessato deve avere la possibilità di **esercitare i propri diritti nei confronti del Titolare**, anche se i suoi dati sono trattati da un responsabile esterno (cloud provider) e in una nuvola informatica. Lo standard obbliga il fornitore ad offrire al Titolare del trattamento, suo cliente, dei tools appropriati che assicurino l'esercizio dei diritti da parte dei soggetti cui i dati si riferiscono.

- il **trattamento è esattamente rispondente a quanto indicato nella policy (informativa)** resa nota all'acquirente dei servizi fin dall'inizio, con esplicita previsione che, nel caso un mutamento di mezzi si rendesse necessario per ragioni tecniche, il cliente ne sia prontamente informato e abbia la facoltà di opporsi oppure uscire dal contratto.

- **i dati personali in cloud non sono trattati per ragioni di marketing diretto o pubblicitarie**, a meno che non vi sia l'esplicito consenso dell'interessato, ma in ogni caso ciò non può mai costituire una precondizione posta dal fornitore al cliente per la fornitura del servizio.

Aspetti principali dello standard ISO 27018 (1/2)

- **i clienti hanno il diritto, fin da subito di conoscere i nomi degli eventuali sub-processors** (intermediari del cloud provider), e il luogo di stabilimento degli stessi, con diritto di opporsi ad eventuali modifiche nella catena dei subfornitori, ovvero dei paesi di loro stabilimento. Può anche essere prevista l'opzione di risolvere il contratto a fronte di tali mutamenti

- **i clienti hanno diritto di ricevere notizia tempestiva delle violazioni di dati personali** (data breaches), al fine di poter a loro volta darne notizia alle autorità di controllo (e agli interessati) nei tempi previsti dalla legge

- siano **disciplinate le modalità di restituzione** dei dati personali al cliente una volta terminato il contratto (cd. transfer back)

- i suoi servizi siano soggetti a **verifiche periodiche di conformità** agli standard di sicurezza, di cui sia fornita evidenza ai clienti

- tutto il suo **personale addetto al trattamento di dati personali sia vincolato da patti di riservatezza** (non disclosure agreements) e riceva adeguata formazione.

Certificazione dei professionisti

In Italia è allo studio una norma (UNI/UNINFO) per la definizione dei profili professionali relativi al trattamento e alla protezione dei dati personali, una professione intellettuale che esercita a diversi livelli di complessità e in diversi contesti organizzativi, pubblici e privati. I profili identificati sono, oltre quello del **Responsabile della protezione dei dati personali** (DPO), il **Manager privacy**, lo **Specialista privacy** e infine il **Valutatore privacy**.

La norma farà riferimento alla Legge 14 gennaio 2013, n. 4, “Disposizioni in materia di professioni non organizzate”.

Ulteriore problema

DELOCALIZZAZIONE TRANSNAZIONALE DEL DATO

conservazione del dato in luoghi geografici differenti

In tal senso il Regolamento UE uniforma il sistema rendendolo omogeneo in casi di storage/trattamento di dati infra UE

inoltre

Il **Regolamento impone** a tutti i soggetti extra UE che trattino dati di cittadini e imprese UE di dover **uniformarsi alle norme del Regolamento** stesso in quanto anch'essi sono potenzialmente sanzionabili:

cd. Principio dello "sportello unico (novità del Regolamento):
consiste nella possibilità per il cittadino europeo di rivolgersi alla propria autorità nazionale di controllo anche nei confronti di trattamenti illeciti dei suoi dati avvenuti su territori extra UE ad opera di soggetti extra UE).

Ancora un problema territoriale…

Cloud Provider e utilizzatore appartenenti a nazionalità e territori diversi

Non potrà escludersi l'applicazione congiunta della normativa nazionale del **Cloud Provider** che potrebbe rivendicarla in relazione al **principio di territorialità nazionale**

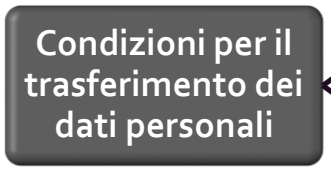
In tal caso occorrerà **individuare la competenza** del giudice (nazionale o straniero) secondo le regole del **diritto internazionale privato** da cui in questa sede dobbiamo prescindere.

Inserire apposite clausole contrattuali

Trasferimenti di dati personali all'estero

20M
4%

Qualunque **trasferimento di dati personali** […] **verso un paese terzo** o **un'organizzazione internazionale**, […], ha luogo **soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni previste dal Regolamento**, applicate al fine di assicurare che il livello di protezione delle persone fisiche non sia pregiudicato.



Decisione di adeguatezza della Commissione

Altre forme di garanzie adeguate

- Strumento giuridicamente vincolante tra autorità pubbliche o organismi pubblici
- Norme vincolanti d'impresa (Binding Corporate Rules – BCR)
- Clausole tipo di protezione dei dati adottate dalla Commissione o adottate da un'autorità di controllo e approvate dalla Commissione

Previa autorizzazione dell'autorità di controllo competente

- Clausole contrattuali tra il titolare o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali
- Accordi amministrativi tra autorità o organismi pubblici

Trasferimenti di dati personali all'estero

20M
4%

Articolo 45

Trasferimento sulla base di una decisione di adeguatezza (C103, C107, C167-C169)

1. Il **trasferimento** di dati personali verso un paese terzo o un'organizzazione internazionale è **ammesso** se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione **garantiscono un livello di protezione adeguato**. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

Decisione di adeguatezza: è un atto della Commissione che certifica che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato secondo i parametri stabiliti dall'art. 45, par. 2.

Revoca della decisione: la Commissione può revocare, modificare o sospendere la decisione di adeguatezza, ma non ha effetto retroattivo (art. 45, par. 5). Quindi, la decisione di revoca o sospensione lascia impregiudicato il trasferimento di dati personali verso il paese terzo, il territorio o uno o più settori specifici all'interno del paese terzo, o verso l'organizzazione internazionale in questione (art. 45, par. 7)

Regime di pubblicità: l'elenco dei paesi terzi, dei territori e dei settori specifici di un paese terzo oggetto di una decisione di adeguatezza sono pubblicate a cura della Commissione sulla Gazzetta ufficiale dell'Unione europea e sul sito web istituzionale.

Trasferimenti di dati personali all'estero

20M
4%

Norme vincolanti d'impresa o «Binding Corporate Rules – BCR» (art. 47)

*Art. 4, n. 20) «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune*

.

Meccanismo di approvazione: Le BCR sono **approvate dall'autorità di controllo** competente secondo il meccanismo di coerenza (art. 63), **con l'intervento del Comitato europeo per la protezione dei dati**.

Contenuti obbligatori (elenco non esaustivo):

- la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;
- i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;
- la loro natura giuridicamente vincolante;
- l'applicazione dei principi generali di protezione dei dati;
- i diritti dell'interessato;
- assunzioni di responsabilità;
- modalità di informazione all'interessato sulle norme vincolanti di impresa;
- i compiti e i ruoli dei soggetti coinvolti nel trattamento;
- le procedure di reclamo;
- i meccanismi interni di verifica della conformità;
- i meccanismi interni per la modifica delle norme, per la cooperazione e segnalazione all'autorità di controllo;
- formazione in materia di protezione dei dati personali

Trasferimenti di dati personali all'estero

20M
4%

Cosa CAMBIA rispetto al passato

Codici di condotta e **schemi di Certificazione**: 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. **Tuttavia**, 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.

Viene meno il requisito dell'autorizzazione nazionale: il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione della Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa potrà avere inizio senza attendere l'autorizzazione nazionale del Garante.

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.

Trasferimenti di dati personali all'estero

20M
4%

Cosa CAMBIA rispetto al passato

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**,

ECCEZIONE a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati.

INOLTRE, sarà 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 – e non dello Stato terzo ricevente.

Trasferimenti di dati personali all'estero

20M
4%

Cosa NON CAMBIA rispetto al passato

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.

Decisioni di adeguatezza della Commissione: Andorra, Argentina, -Australia – PNR, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA-Privacy Shield e USA-PNR

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, sino a loro eventuale modifica.

Il consenso

In base alla disciplina generale è essenziale

- il **consenso (informato) dell'interessato al trattamento** (il proprietario dei dati), che dovrà essere il più amplio possibile anche in relazione alla conservazione effettuata con nuovi strumenti tecnologici (anche in cloud)
- **Il consenso del titolare del trattamento** (il cliente del provider) a spostare e delocalizzare geograficamente i dati in altre località transazionali

Inserire apposite clausole contrattuali tra Cloud Provider e cliente che dovranno tener conto dell'impatto normativo e dei livelli di sicurezza

Le misure di sicurezza

si distinguono in due principali tipologie:

Misure tecniche

Misure organizzative

Tutto l'impianto normativo del Regolamento è basato sul **principio della «responsabilizzazione»** (*accountability*) di titolari e responsabili. 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.

Le misure di sicurezza

10M
2%

Sicurezza del trattamento (art. 32)

Titolare del trattamento e Responsabile del trattamento

…attuano **misure tecniche** e **organizzative adeguate** per garantire **un livello di sicurezza adeguato al rischio**…attuano **misure tecniche** e **organizzative adeguate** per garantire **un livello di sicurezza adeguato al rischio**

tenendo conto:
- dello stato dell'arte
- dei costi di attuazione
- della natura, dell'oggetto, del contesto e delle finalità del trattamento,
- del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

Valutazione dei rischi

La valutazione dei rischi era **già prevista dalla disciplina del D.lgs. 196/03.**
Oggi acquista **maggiore importanza** e **rilevanza** in quanto rappresenta la base da cui partire per sviluppare **ogni tipo di misura tecnica** e **organizzativa** per garantire la **sicurezza** dei dati personali.

Non esiste più la distinzione misure minime di sicurezza / misure idonee di sicurezza.

Con il nuovo regolamento, **tutte le misure di sicurezza devono essere adottate in seguito ad una valutazione dei rischi**. Non esiste più un nucleo minimo di misure di sicurezza che se venivano rispettate il titolare era al sicuro da eventuali sanzioni.

Valutazione del rischio per i diritti e le libertà delle persone fisiche

- Cosa si intende per rischi
- Quando possono sorgere i rischi
- Quali sono gli eventi che costituiscono il fattore di rischio
- Come valutare i rischi

La scelta delle misure tecniche e organizzative per la sicurezza dei dati personali

- Quando le misure tecniche e organizzative sono adeguate al rischio
- Come effettuare la scelta delle misure da adottare

Grazie per l'attenzione

Massimo Farina

http://www.massimofarina.it/

http://www.diricto.it/

http://ict4forensics.diee.unica.it/

massimo@massimofarina.it

Licenza

creative commons
COMMONS DEED

Attribuzione - Non Commerciale - Condividi allo stesso modo 4.0 (CC BY-NC-SA 4.0) Internazionale

- **Tu sei libero di:**

  Condividere - riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare questo materiale con qualsiasi mezzo e formato;

  Modificare - remixare, trasformare il materiale e basarti su di esso per le tue opere;

Il licenziante non può revocare questi diritti fintanto che tu rispetti i termini della licenza

Alle seguenti condizioni:

- **Attribuzione**. Devi riconoscere una menzione di paternità adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare ciò in qualsiasi maniera ragionevole possibile, ma non con modalità tali da suggerire che il licenziante avalli te o il tuo utilizzo del materiale.
- **Non commerciale**. Non puoi usare il materiale per fini commerciali.
- **Stessa Licenza**. Se remixi, trasformi il materiale o ti basi su di esso, devi distribuire i tuoi contributi con la stessa licenza del materiale originario.

- **Divieto di restrizioni aggiuntive** — Non puoi applicare termini legali o misure tecnologiche che impongano ad altri soggetti dei vincoli giuridici su quanto la licenza consente loro di fare.
- Non sei tenuto a rispettare i termini della licenza per quelle componenti del materiale che siano in pubblico dominio o nei casi in cui il tuo utilizzo sia consentito da una eccezione o limitazione prevista dalla legge
- Non sono fornite garanzie. La licenza può non conferirti tutte le autorizzazioni necessarie per l'utilizzo che ti prefiggi. Ad esempio, diritti di terzi come i diritti all'immagine, alla riservatezza e i diritti morali potrebbero restringere gli usi che ti prefiggi sul materiale.