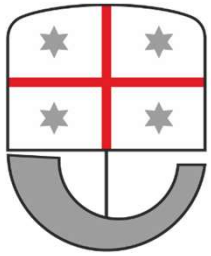


Liguria Digitale

Trasferimenti dei dati personali extra UE post sentenza Schrems II

Linux Day 23 ottobre 2021

Nicola Faravelli & Maurizio Pastore

LIGURIA DIGITALE

Liguria Digitale, società ICT **in house** della Regione Liguria, lavora anche per il mercato, proponendo **soluzioni** e **infrastrutture tecnologiche** e **servizi digitali rivolti** a **imprese ed enti.**

GDPR COMPETENCE CENTRE

Il **GDPR** Competence Center di Liguria Digitale è un **team di esperti** che supporta **aziende ed enti**, dalla fase di **progettazione** by design & by default alla **gestione** dei **dati**.

Chi sono e cosa faccio

Nicola Faravelli

- Giurista, 30 anni
- Focalizzato su Privacy e diritto amministrativo
- Da 2 anni segue gli sviluppi sw di uno strumento per la compliance GDPR
- Sono RPD di alcuni Enti (Comuni, ARPAL) e associazioni di volontariato
- Per contattarmi n.faravelli(at)liguriadigitale.it
- Servizi GDPR Liguria Digitale

Chi sono e cosa faccio

Maurizio Pastore

- Ingegnere, 60 anni, amante della natura
- Lavoro su Unix, Linux dal 1984
- Lavoro sempre in ambito ICT
- Ultimamente (2012) mi occupo di:
  - Sicurezza Informativa
  - Privacy: sono RPD di numerosi Enti (AOU, ASL, Comuni) e sanità convenzionata
  - Cloud
- Per contattarmi m.pastore(at)liguriadigitale.it
- Servizi GDPR Liguria Digitale

Oggi parliamo di…

1. Cos'è un trasferimento di dati personali
2. Principi generali e quadro normativo di riferimento
3. Sentenza Schrems II
4. Panorama e incertezze post Sentenza

Definizione di trasferimento

Il Regolamento europeo 679/2016 (GDPR) non contiene una definizione puntuale di trasferimento ma la si può ricavare implicitamente da altre definizioni

Definizione di trasferimento

Art. 4 GDPR: «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la **comunicazione mediante trasmissione**, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

Definizione di trasferimento

Considerando 101: «…È opportuno però che, quando i dati personali sono **trasferiti** dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso…»

Quindi, si esegue un trasferimento quando i dati personali **sono trasferiti verso un destinatario soggetto a una giurisdizione straniera (extra UE)**

Definizione di trasferimento

Il trasferimento avviene anche quando viene eseguito un accesso (consultazione) da un paese terzo verso una banca dati situata all'interno dell'UE.

Quindi dire che i server sono in SEE NON BASTA:

- Occorre individuare se ai server hanno accesso, per motivi operativi o normativi, soggetti situati extra SEE

Definizione di trasferimento

Ma la pubblicazione su un sito internet costituisce un trasferimento?

Secondo la Corte di Giustizia europea, a seguito della **sentenza Lindqvist** la semplice **pubblicazione di dati personali su un sito Internet** non può considerarsi trasferimento all'estero, in quanto tale trasferimento avverrebbe necessariamente verso tutti i paesi esteri e quindi il regime speciale stabilito per i flussi transfrontalieri finirebbe per diventare un regime generale.

Principi Generali e quadro normativo

Considerando 102: Gli Stati membri possono concludere **accordi internazionali** che implicano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, purché tali accordi non incidano sul GDPR o su qualsiasi altra disposizione del diritto dell'Unione e includano un **adeguato livello di protezione per i diritti fondamentali degli interessati.**

Principi Generali e quadro normativo

Considerando 116: Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per **tutelarsi da usi o comunicazioni illeciti di tali informazioni**. […] Pertanto vi è la necessità di promuovere una più stretta **cooperazione tra le autorità di controllo** della protezione dei dati affinché possano scambiare informazioni e condurre indagini di concerto con le loro controparti internazionali

Principi Generali e quadro normativo

Art. 1, par. 3: La **libera circolazione dei dati personali nell'Unione non può essere limitata né vietata** per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Art. 3, par 1: Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito **delle attività di uno stabilimento** da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, **indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione**

Principi Generali e quadro normativo

Art. 44: **Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento** verso un paese terzo o un'organizzazione internazionale, **compresi trasferimenti successivi** di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di **assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato**

Trasferimento attraverso una decisione di adeguatezza

Art 45, par. 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**

Trasferimento attraverso una decisione di adeguatezza

Art 45, par. 2: Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi:

a) lo **stato di diritto**, il **rispetto dei diritti umani e delle libertà fondamentali**, la **pertinente legislazione generale e settoriale** (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le **norme in materia di protezione dei dati**, le norme professionali e le misure di sicurezza […]

b) l'esistenza e l'effettivo funzionamento di una o più **autorità di controllo indipendenti nel paese terzo** […]

c) gli **impegni internazionali assunti** dal paese terzo […]

Trasferimento attraverso una decisione di adeguatezza

Art 45, par. 3: La **Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione**, 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** ai sensi del paragrafo 2 del presente articolo.

L'atto di esecuzione prevede un meccanismo di **riesame periodico, almeno ogni quattro anni**, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale

Trasferimento attraverso una decisione di adeguatezza

Art 45, par. 5: Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale **non garantiscono più un livello di protezione adeguato**, la **Commissione revoca, modifica o sospende nella misura necessaria la decisione del presente articolo mediante atti di esecuzione senza effetto retroattivo**

Trasferimento attraverso una decisione di adeguatezza

La Commissione europea finora (13 novembre 2020) ha riconosciuto l'adeguatezza dei seguenti Stati:

Andorra, Argentina, Canada (organizzazioni commerciali), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay ~~e gli Stati Uniti d'America (solo chi iscritto al Privacy Shield)~~

(https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy- decisions_en)

La sentenza C-311/18 (Schrems II)

La Corte ha esaminato la validità della decisione relativa allo «scudo per la privacy» (Decisione 2016/1250 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy), poiché i trasferimenti in questione nel contesto della controversia nazionale sfociata nella domanda di pronuncia pregiudiziale hanno avuto luogo tra l'UE e gli Stati Uniti («USA»).

La sentenza C-311/18 (Schrems II)

Secondo la Corte, i requisiti della normativa interna degli Stati Uniti, e in particolare **taluni programmi che consentono l'accesso da parte delle autorità pubbliche statunitensi**, **per finalità di sicurezza nazionale, ai dati personali trasferiti dall'Unione europea verso gli Stati Uniti**, comportano limitazioni della protezione dei dati personali che non sono configurate in modo da soddisfare requisiti sostanzialmente equivalenti a quelli richiesti nel diritto dell'Unione; inoltre, tale normativa **non conferisce agli interessati diritti azionabili in sede giudiziaria nei confronti delle autorità statunitensi**. Alla luce di tale grado di **ingerenza nei diritti fondamentali** delle persone i cui dati sono trasferiti verso tale paese terzo, la Corte ha dichiarato invalida la decisione sull'adeguatezza dello scudo per la privacy.

La sentenza C-311/18 (Schrems II)

In generale, per i paesi terzi, la soglia fissata dalla Corte si applica anche a tutte le garanzie adeguate di cui all'articolo 46 del RGPD, utilizzate per il trasferimento dei dati dal SEE a qualsiasi paese terzo. La normativa statunitense richiamata dalla Corte [l'articolo 702 del Foreign Intelligence Surveillance Act (FISA) e l'Executive Order (EO) 12333] si applica a qualsiasi trasferimento verso gli Stati Uniti eseguito con mezzi elettronici che rientri nell'ambito di applicazione della suddetta normativa, a prescindere dallo strumento utilizzato per il trasferimento.

La sentenza C-311/18 (Schrems II)

Cosa sono la FISA e l'EO 12333?

Ai sensi della FISA (Sezione 702), i "fornitori di servizi di comunicazione elettronica" statunitensi (come definiti nel 50 U.S.C. §1881(4)) possono essere obbligati a concedere alle autorità di sicurezza statunitensi l'accesso ai dati personali di "persone non statunitensi", definite come chiunque non sia cittadino statunitense o residente permanente negli Stati Uniti. **Gli ordini** di sorveglianza previsti da questa legge **non devono essere specifici** per un singolo obiettivo, ma consentono piuttosto un intero programma di **sorveglianza a tappeto**.

La sentenza C-311/18 (Schrems II)

Chi sono i fornitori di servizi di comunicazione elettronica?

- vettore di telecomunicazioni (telecommunication carrier);
- fornitore di servizi di comunicazione elettronica;
- fornitore di servizi di elaborazione remota;
- qualsiasi altro fornitore di servizi di comunicazione che abbia accesso a comunicazioni via cavo o elettroniche in quanto tali comunicazioni vengono trasmesse o quando tali comunicazioni vengono archiviate e qualsiasi funzionario, dipendente o agente di tale fornitore.

La sentenza C-311/18 (Schrems II)

Quindi chi è escluso da questa categoria?

Aziende, come banche, compagnie aeree, hotel, compagnie di navigazione, vendite di beni e simili non sono soggette a tali norme, per cui in teoria non si dovrebbe porre alcun problema nell'utilizzarle quali fornitori di servizi. Ovviamente può, però, accadere, che una banca o un hotel utilizzi un fornitore di servizi di comunicazione elettronica, nel qual caso le agenzie Usa possono accedere ai dati trasferiti, e questo rende la tutela "non adeguata" con tutte le conseguenze del caso.

NB: la "sorveglianza" delle agenzie americane si realizza anche nel corso della trasmissione dei dati (in transito o *upstream*). In tale prospettiva occorre che chi trasferisce i dati si assicuri che siano cifrati, in tal modo ottemperando alle previsioni di cui all'art. 32 del GDPR.

La sentenza C-311/18 (Schrems II)

Che cos'è l'Executive Order (EO) 12333?

All'origine delle attività di controllo da parte del governo statunitense c'è una **base giuridica**, **l'Ordine esecutivo 12333** (EO 12333) che **risale al 1981, durante la presidenza di Ronald Reagan.**

Concede alle agenzie di intelligence **una grande libertà di manovra** nel raccogliere e gestire enormi di quantità di dati americani. Come reso pubblico con lo **scandalo Datagate**, oggi queste informazioni possono andare dai contenuti della **posta elettronica** ai **messaggi di Facebook**, dalle **chiamate su Skype**

La sentenza C-311/18 (Schrems II)

Cos'è il Cloud ACT?

il **Cloud Act** consente alle autorità statunitensi, forze dell'ordine e agenzie di intelligence di **acquisire dati informatici dagli operatori di servizi di cloud computing** a prescindere dal posto dove questi dati si trovano; quindi anche se sono su server fuori dagli Usa. La sola condizione è che questi operatori siano **sottoposti alla giurisdizione degli Stati Uniti** oppure anche – attenzione – siano **le società europee che hanno una filiale negli Stati Uniti o che operano nel mercato americano.**

La sentenza C-311/18 (Schrems II)

Da cosa ha origine il Cloud ACT?

il CLOUD Act ha tratto origine anche da una nota disputa del 2013, in cui il Federal Bureau of Investigation (FBI), ai sensi dello Stored Communications Act del 1986 (SCA), chiese l'accesso alle informazioni presenti nei server di **Microsoft** situati in Irlanda. Microsoft si oppose, affermando che lo Stored Communications Act (SCA) del 1986, su cui era basata la richiesta, non si applicava ai dati ubicati al di fuori del territorio degli Stati Uniti. **Prima che il caso venisse deciso, fu adottato il CLOUD Act**

La sentenza C-311/18 (Schrems II)

Cos'altro ha precisato la Corte?

La decisione 2010/87/UE stabilisce **l'obbligo** per l'esportatore dei dati e il destinatario di tali dati (l'"importatore dei dati") di verificare, preliminarmente al trasferimento, e tenendo conto delle circostanze di quest'ultimo, se il livello di protezione sia rispettato nel paese terzo considerato. Inoltre, la Corte rileva che la decisione 2010/87/UE impone all'importatore dei dati di informare l'esportatore di qualsiasi impossibilità di conformarsi alle clausole tipo di protezione nonché, ove necessario, a eventuali misure supplementari a quelle offerte dalle clausole, con l'onere, in tal caso, per l'esportatore dei dati di sospendere il trasferimento di dati e/o di risolvere il contratto concluso con l'importatore

La sentenza C-311/18 (Schrems II)

Si possono utilizzare le BCR?

In considerazione della sentenza della Corte, che ha invalidato lo scudo per la privacy a causa del grado di ingerenza creato dalla normativa statunitense nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo, e alla luce della circostanza per cui lo scudo per la privacy è stato concepito anche per fornire garanzie ai dati trasferiti con altri strumenti, quali le norme vincolanti d'impresa, la valutazione della Corte si applica anche nel contesto delle norme vincolanti d'impresa, poiché la normativa statunitense prevarrà anche su quest'ultimo strumento. La possibilità di trasferire i dati personali sulla base delle norme vincolanti d'impresa dipenderà dal risultato della valutazione effettuata, tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili.

Segue…

Tali misure supplementari unitamente alle norme vincolanti d'impresa, previa analisi caso per caso delle circostanze del trasferimento, dovrebbero assicurare che la normativa statunitense non interferisca con il livello di protezione adeguato dalle stesse garantito. Qualora si giunga alla conclusione che, tenuto conto delle circostanze del trasferimento e delle possibili misure supplementari, non sarebbero assicurate garanzie adeguate, vi è l'obbligo di sospendere o cessare il trasferimento dei dati personali. Se si intende ciononostante proseguire col trasferimento dei dati, è obbligatorio informare l'autorità di controllo competente

Trasferimento **in assenza** di decisioni di adeguatezza

Quali alternative per eseguire un trasferimento lecito in USA (e non solo)?

Senza decisioni di adeguatezza il processo è complicato e richiede conoscenze elevate

EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

1. Individuare i trasferimenti effettuati (direttamente **o da propri Responsabili/sub Responsabili**)
2. Individuare il meccanismo di trasferimento
3. Verificare le norme applicabili **e applicate per equivalenza**
4. Individuare misure aggiuntive
5. Documentare le decisioni (SCC, BCR, ect.)
6. Rivedere periodicamente

Misure supplementari tecniche applicabili

Tendono a trasformare il dato personale in un dato anonimo:

- Cifratura effettuata prima della trasmissione e conservazione: esempio copia di backup cifrato in Italia dal Titolare su sistemi propri
- Forte Pseudonimizzazione: Applicazione prima della trasmissione fuori SEE delle tecniche presentate https://www.linuxday.it/2021/programma/talk.php?slug=deidentificazione-dei-dati-personali-al-tempo-del-gdpr

Misure supplementari organizzative

- Consegnare i dati in chiaro solo a soggetti che possano opporre alle autorità una effettiva negazione dell'accesso:
  - Operatori sanitari
  - Sedi diplomatiche
- Tali organizzazioni fidate devono a loro volta operare per trattare i dati in modo tale che non ci sia possibilità di accesso da parte delle autorità non adeguate:
  - Trasmettere solo dati cifrati (ove gli ISP sono obbligati a intercettare)
  - Non usare servizi Cloud

Trasferimento **in assenza** di decisioni di adeguatezza

Art. 46, par. 1: In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale **solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi**

Trasferimento **in assenza** di decisioni di adeguatezza

Art. 46, par. 2: Possono costituire **garanzie adeguate senza necessitare di autorizzazioni specifiche** da parte di un'autorità di controllo:

a) uno **strumento giuridicamente vincolante** e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici
b) le **norme vincolanti d'impresa**
c) le **clausole tipo di protezione dei dati adottate dalla Commissione**
d) le **clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione**
e) un **codice di condotta approvato**
f) un **meccanismo di certificazione**

Trasferimento **in assenza** di decisioni di adeguatezza

Art. 46, par. 3: Fatta **salva l'autorizzazione dell'autorità di controllo competente**, possono altresì **costituire garanzie adeguate**:

a) le **clausole contrattuali** tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale

b) le **disposizioni da inserire in accordi amministrativi** tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati

Le clausole contrattuali standard

Art. 46, par. 5: **Le autorizzazioni rilasciate** da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della direttiva 95/46/CE **restano valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo**. Le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata conformemente al paragrafo 2 del presente articolo

Le clausole contrattuali standard

L'azienda o il soggetto pubblico può **accordarsi con la controparte nel paese terzo per utilizzare le Clausole-tipo di protezione dati approvate dalla Commissione europea**

Con tali clausole si possono prestare le **garanzie adeguate in termini di protezione dati** che sono richieste qualora si trasferiscano dati personali verso un paese terzo

Le clausole contrattuali standard

Strutturazione (indicativa) dei contratti di trasferimento attraverso **clausole standard**:

- Definizioni - Descrizione del trasferimento Clausola del terzo beneficiario
- Obblighi dell'esportatore – Obblighi dell'importatore
- Responsabilità - Diritti dei terzi
- Mediazione e giurisdizione - Collaborazione con le autorità di controllo Legge applicabile – Modifica del contratto
- Subcontratto
- Obblighi al termine dell'attività di trattamento dei dati personali

Le clausole contrattuali standard

È importante sottolineare che le clausole-tipo di protezione dati **non ammettono emendamenti e devono essere sottoscritte dalle parti**

Tuttavia, esse possono essere incorporate in un contratto più generale e vi **si possono aggiungere clausole ulteriori purché non in conflitto**, direttamente o indirettamente, con le clausole-tipo approvate dalla Commissione europea

Le clausole contrattuali standard

Ogni ulteriore modifica o emendamento delle clausole-tipo ne comporta la **trasformazione in clausole contrattuali ad-hoc**. Anche queste ultime possono offrire garanzie adeguate

Prima di procedere al trasferimento, queste clausole contrattuali speciali necessitano **dell'autorizzazione della competente autorità di controllo nazionale, preceduta in ogni caso dal parere del Comitato europeo della protezione dei dati**

Deroghe in specifiche situazioni

Art. 49: In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, **è ammesso il trasferimento** o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale **soltanto se si verifica una delle seguenti condizioni**:

a) l'interessato abbia **esplicitamente acconsentito al trasferimento proposto**, dopo essere stato **informato dei possibili rischi** di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate […]

Deroghe in specifiche situazioni

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato

d) il trasferimento sia necessario per importanti motivi di interesse pubblico […]

Deroghe in specifiche situazioni

e) il il trasferimento sia **necessario per accertare, esercitare o difendere un diritto in sede giudiziaria**

f) il trasferimento sia necessario per **tutelare gli interessi vitali dell'interessato o di altre persone**, qualora l'interessato si trovi **nell'incapacità fisica o giuridica di prestare il proprio consenso**

g) il trasferimento sia **effettuato a partire da un registro che**, a norma del diritto dell'Unione o degli Stati membri, **mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse**, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membro

Deroghe in specifiche situazioni

Se non è possibile basare il trasferimento su una disposizione dell'articolo 45 o 46, comprese le disposizioni sulle norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni a norma del primo comma del presente paragrafo è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale sia **ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali**

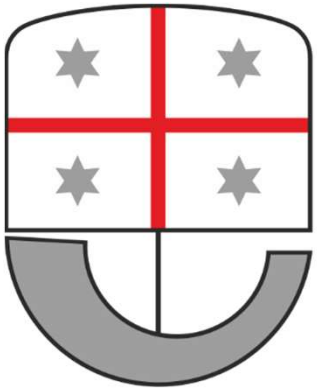
Deroghe in specifiche situazioni

Art. 49, par. 3: le lettere a), b) e c)del paragrafo 1 non si applicano alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

Quindi le deroghe specifiche possono essere utilizzate da realtà private e non pubbliche (sostanzialmente il principio opposto a quello USA)

Sanzioni

- Garante Italiano: Università bocconi: 200k€ per aver utilizzato un fornitore americano per esami on line
- Garante Portoghese: Raccomanda di non usare
- Garante Bavarese: l'Autorità tedesca ha considerato illegittimo il trasferimento di dati personali extra UE effettuato dalla società tedesca FOGS Magazin che si avvaleva dei servizi Mailchimp in materia di newsletter



Liguria Digitale

Grazie dell'attenzione