UNIVERSITÁ DEGLI STUDI DI TERAMO

Cloud e strumenti collaborativi

Roberto Salvatori
Università di Teramo

Cloud Computing:
Cenni ad aspetti legislativi
Quarta parte

IV. Aspetti legislativi del trattamento dei dati su Cloud ed Infrastrutture di Calcolo e Storage distribuite

Aree di legislazione interessate dal Cloud

- Protezione e Sicurezza dei dati in generale
- Aspetti legati alla competizione/competitività
- Libertà di espressione
- Protezione della proprietà intellettuale
- ...

Definizione di Dati Personali

Cosa sono i Dati Personali ?

Dati

+ una persona fisica

+ una relazione (anche indiretta) tra loro

= Dati Personali

Quadro di riferimento EU normativo e strategico

- Direttiva EU 95/46/CE sulla protezione dei dati personali – 24 Ottobre 1995
- Direttiva EU 2002/58/EC sull' e-Privacy – 12 Luglio 2002
- Comunicazione 2010 (609) Un approcio globale alla protezione dei dati personali nell' Unione Europea – 4 Novembre 2010
- Comunicazione 2012 (11) Proposta della Commissione EU di una regolamentazione da parte del Parlamento e del Consiglio Europeo sulla protezione di cittadini rispetto al processamento dei dati personali e sulla loro libera circolazione (*General Data Protection Regulation*) – 25 Gennaio 2012
- Opinione (Opinion 05/2012) sul Cloud Computing adottata dal Gruppo di lavoro EU Article 29 Working Party – 1 Luglio 2012
- EU Memo 2012/713 e Comunicazione 2012/529 "Unleashing the potential of Cloud Computing in Europe" - 27 Settembre 2012

NON ESAUSTIVO

Articolo 29 della Direttiva 95/46/CE

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

1. **È istituito un gruppo per la tutela della persone con riguardo al trattamento dei dati personali**, in appresso denominato «il gruppo».

Il gruppo ha carattere consultivo e indipendente.

2. Il gruppo è **composto da**
    1. un rappresentante della o **delle autorità di controllo designate da ciascuno Stato membro**
    2. da un rappresentante della o delle **autorità create per le istituzioni e gli organismi comunitari**,
    3. da un rappresentante della **Commissione.**

Ogni membro del gruppo è designato dall'istituzione oppure dalla o dalle autorità che rappresenta. Qualora uno Stato membro abbia designato più autorità di controllo, queste procedono alla nomina di un rappresentante comune. Lo stesso vale per le autorità create per le istituzioni e gli organismi comunitari.

3. **Il gruppo adotta le sue decisioni alla maggioranza semplice** dei rappresentanti delle autorità di controllo.

4. Il gruppo elegge il proprio presidente. **La durata del mandato del presidente è di due anni**. Il mandato è rinnovabile.

5. Al segretariato del gruppo provvede la Commissione.

6. Il gruppo **adotta il proprio regolamento interno**.

7. Il gruppo esamina le questioni iscritte all'ordine del giorno dal suo presidente, su iniziativa di questo o su richiesta di un rappresentante delle autorità di controllo oppure su richiesta della Commissione.

Articolo 30 della Direttiva 95/46/CE

- 1. **Il gruppo ha i seguenti compiti:**
  - a) **esaminare ogni questione attinente all'applicazione delle norme nazionali** di attuazione della presente direttiva per contribuire alla loro applicazione omogenea;
  - b) **formulare, ad uso della Commissione, un parere sul livello di tutela** nella Comunità e nei paesi terzi;
  - c) **consigliare la Commissione in merito a ogni progetto di modifica della presente direttiva,** ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali, nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano su tali diritti e libertà;
  - d) **formulare un parere sui codici di condotta** elaborati a livello comunitario.
- 2. Il gruppo, **qualora constati che tra le legislazioni o prassi degli Stati membri si manifestano divergenze** che possano pregiudicare l'equivalenza della tutela delle persone in materia di trattamento dei dati personali nella Comunità, **ne informa la Commissione.**
- 3. Il gruppo **può formulare di propria iniziativa raccomandazioni su qualsiasi questione riguardante la tutela delle persone** nei confronti del trattamento di dati personali nella Comunità.
- 4. I pareri e le raccomandazioni del gruppo vengono trasmessi alla Commissione e al comitato di cui all'articolo 31.
- 5. **La Commissione informa il gruppo del seguito da essa dato** ai pareri e alle raccomandazioni. A tal fine redige una relazione che viene trasmessa anche al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione.
- 6. Il gruppo **redige una relazione annuale** sullo stato della tutela delle persone fisiche con riguardo al trattamento dei dati personali nella Comunità e nei paesi terzi e la trasmette alla Commissione, al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione.

Rischi del Cloud Computing: Mancanza di Controllo

(opinion 05/2012 Art.29 WP)

- Mancanza di disponibilità dei dati
  - a causa della mancanza di interoperabilità (**vendor lock-in**)
- Mancanza di integrità causato dalla condivisione delle risorse:
  - Una Cloud è composta da comune sistemi e infrastrutture.
- Mancanza di riservatezza
  - in termini di richieste di applicazione di legge effettuate direttamente a un Cloud provider
- Mancanza di possibilità di intervento
  - causa della complessità e della dinamica della catena di outsourcing / sottofornitori
- Mancanza di possibilità di intervento (esercitare i diritti dell'interessato):
  - Un Cloud provider può non fornire le misure e gli strumenti necessari per assistere il controller per gestire i dati in termini di, ad esempio, l'accesso, la cancellazione o la correzione dei dati.
- Mancanza di isolamento:
  - un provider di cloud può usare il suo controllo fisico sui dati da diversi client per collegare i dati personali.

Mancanza di Informazione sul processamento dei dati

- **Mancanza di informazioni sul processamento dei dati (Trasparenza)**

La mancanza di informazioni sulle operazioni di processamento dati di un servizio Cloud rappresenta un rischio sia per il Controllore dei Dati che per i Cittadini (Data Subjects) perchè possono non essere al corrente di minacce potenziali e rischi e perciò possono non essere in grado di adottare le misure correttive necessarie

- **Minacce relative al Controller dei dati che non sia al corrente del fatto che**:
  - Il processamento a catena dei dati avviene coinvolgendo più di un Processore dei Dati e Subcontrators.
  - I Dati Personali sono processati in aree geografiche distinte nello SEE (EEA) – Spazio Economico Europeo.
    - quale legislazione applicare in caso di disputa sui Dati Personali che possa nascere tra utente e provider?
  - I Dati sono trasferiti verso paesi terzi al di fuori dello SEE.
    - Paesi terzi possono non fornire un livello di protezione adeguato ed I trasferimenti possono non essere tutelati da misure adeguate (es.clausole contrattuali standard o regole aziendali stringeti) – e quindi possono essere illegali

- Si richiede che I cittadini I cui dati Personali sono processati nella Cloud **siano informati dell' identità del data controller e degli scopi del processamento dei dati** *(un requirement che esiste per tutti i Controllori secondo la Data Protection Directive 95/46/EC).*

- Data la potenziale complessità delle catene di processamento dati in ambiente Cloud, per garantire un processamento corretto per rispetto ai cittadini (Articolo 10 della Direttiva 95/46/EC**), i controller devono di norma fornire ulteriori informazioni relative ai (sub-)processori che forniscono il servizio Cloud**.

Rischi del Cloud Computing relativamente al trattamento dei Dati Personali: Riepilogo

(Opinion 05/2012 Art.29 WP)

da: diritto.it

Riassunto Opinion 05/2012 Art.29 WP

Contesto legislativo EU per la protezione dei dati:

95/46/EC	2002/58/EC

Legge applicabile:

quella del paese(i) ove il Cliente/Titolare è stabilito

Rapporto Cliente-Fornitore-Subfornitori

Essenziale stabilire:
- la ripartizione delle responsabilità per la conformità alla legge
- come consentire in pratica l'esercizio dei diritti degli Interessati

Principi basilari

Trasparenza	Trattamenti limitati alle finalità consentite	Conservazione dati/cancellazione dei dati
• tra Cliente ed Interessati • tra Cliente e Fornitore Chiarezza e completezza nel contratto	Rischi dalla presenza di molti Fornitori/Subfornitori Misure tecniche/organizzative e obbligazioni contrattuali	Necessaria certezza nelle operazioni Misure tecniche/organizzative e obbligazioni contrattuali

Tutele contrattuali, trasferimenti di dati all'estero

- Necessario stabilire un contratto tra Cliente e Fornitore
- Trasferimento di dati verso paesi extra EEA:
  - In generale non applicabili i casi di esenzione previsti dalla 95/46/EC
  - Safe Harbour per i fornitori U.S.A. (comunque per i servizi cloud è opportuno assessment da terza parte)
  - in generale da preferire le clausole contrattuali standard stabilite dalla UE (es. 2010/87/UE) e/o Binding Corporate rules

Misure tecnico-organizzative:

Disponibilità dei dati:	Back-up dei dati e procedure di ripristino /Ridondanza di base dati Adeguate caratteristiche del servizio Internet utilizzato
Integrità dei dati:	Intrusion Detection/prevention Systems, Meccanismi di autentificazione crittografica
Riservatezza dei dati:	Dati crittografati sia in "transito" sulla rete sia quando "residenti" sui server Meccanismi di strong authentication per gli utenti (*)
Trasparenza:	Chiarezza e completezza nel contratto
Trattamenti limitati alle finalità consentite	Governance nella distribuzione e nel controllo dei diritti di accesso ai dati personali (*) e Relative misure tecniche
Corrispondere alle richieste di Esercizio dei diritti:	Obligazioni contrattuali che assicurino al Cliente il supporto del Fornitore (e Subfornitori)
Portabilità dei dati (compatibilità con altri Fornitori-Sistemi)	Verifiche precontrattuali e Obligazioni contrattuali che assicurino la portabilità al termine del Contratto con il Fornitore (quale ne sia il motivo)
Accountability: *In ambito Information Technology: capacità di stabilire cosa è stato fatto e come in un determinato tempo In ambito protezione dati: la capacità di dimostrare che sono stati prese le appropriate misure ai fini della conformità alla normativa*	Sono richieste misure tecnico-organizzative per dimostrare l'esistenza di una privacy-security Policy e la sua effettiva implementazione, incluse eventuali certificazioni emesse da terze parti. Necessarie apposite obligazioni contrattuali E' essenziale per consentire al Cliente di corrispondere alle richieste delle autorità competenti (DPA) previste dalla legge *(ad esempio per il caso di "violazione dei dati personali" nei servizi di comunicazione elettronica accessibili al pubblico, introdotto in Italia dal D.Lgs 69/12)*

da: diritto.it

WP 29 Opinion 5/12: riepilogo dei principali aspetti del contesto normativo e delle misure individuate

Contesto legislativo EU per la protezione dei dati:	
95/46/EC	2002/58/EC

Legge applicabile:
quella del paese(i) ove il Cliente/Titolare è stabilito

Rapporto Cliente-Fornitore-Subfornitori
Essenziale stabilire: • la ripartizione delle responsabilità per la conformità alla legge • come consentire in pratica l'esercizio dei diritti degli Interessati

Principi basilari

Trasparenza	Trattamenti limitati alle finalità consentite	Conservazione dati/cancellazione dei dati
• tra Cliente ed Interessati • tra Cliente e Fornitore Chiarezza e completezza nel contratto	Rischi dalla presenza di molti Fornitori/Subfornitori Misure tecniche/organizzative e obligazioni contrattuali	Necessaria certezza nelle operazioni Misure tecniche/organizzative e obligazioni contrattuali

Tutele contrattuali, trasferimenti di dati all'estero
•Necessario stabilire un contratto tra Cliente e Fornitore •Trasferimento di dati verso paesi extra EEA: •In generale non applicabili i casi di esenzione previsti dalla 95/46/EC •Safe Harbour per i fornitori U.S.A. (comunque per i servizi cloud è opportuno assessment da terza parte) • in generale da preferire le clausole contrattuali standard stabilite dalla UE (es. 2010/87/UE) e/o Binding Corporate Rules

Misure tecnico-organizzative:	
Disponibilità dei dati:	Back-up dei dati e procedure di ripristino /Ridondanza di base dati Adeguate caratteristiche del servizio Internet utilizzato
Integrità dei dati:	Intrusion Detection/prevention Systems, Meccanismi di autentificazione crittografica
Riservatezza dei dati:	Dati crittografati sia in "transito" sulla rete sia quando "residenti" sui server Meccanismi di strong authentication per gli utenti (*)
Trasparenza:	Chiarezza e completezza nel contratto
Trattamenti limitati alle finalità consentite	Governance nella distribuzione e nel controllo dei diritti di accesso ai dati personali (*) e Relative misure tecniche
Corrispondere alle richieste di Esercizio dei diritti:	Obligazioni contrattuali che assicurino al Cliente il supporto del Fornitore (e Subfornitori)
Portabilità dei dati (compatibilità con altri Fornitori-Sistemi)	Verifiche precontrattuali e Obligazioni contrattuali che assicurino la portabilità al termine del Contratto con il Fornitore (quale ne sia il motivo)
Accountability: *In ambito Information Technology capacità di stabilire cosa è stato fatto e come in un determinato tempo* *In ambito protezione dati la capacità di dimostrare che sono stati prese le appropriate misure ai fini della conformità alla normativa*	Sono richieste misure tecnico-organizzative per dimostrare l'esistenza di una privacy-security Policy e la sua effettiva implementazione, incluse eventuali certificazioni emesse da terze parti. Necessarie apposite obligazioni contrattuali E' essenziale per consentire al Cliente di corrispondere alle richieste delle autorità competenti (DPA) previste dalla legge *(ad esempio per il caso di "violazione dei dati personali" nei servizi di comunicazione elettronica accessibili al pubblico, introdotto in Italia dal D.Lgs 69/12)*

(*) presso il Fornitore, i Subfornitori, ..ed il Cliente

da: diritto.it

Riassunto Opinion 05/2012 Art.29 WP

Contesto legislativo EU per la protezione dei dati:	
95/46/EC	2002/58/EC

Legge applicabile:
quella del paese(i) ove il Cliente/Titolare è stabilito

Rapporto Cliente-Fornitore-Subfornitori
Essenziale stabilire: • la ripartizione delle responsabilità per la conformità alla legge • come consentire in pratica l'esercizio dei diritti degli Interessati

Principi basilari		
Trasparenza	Trattamenti limitati alle finalità consentite	Conservazione dati/cancellazione dei dati
• tra Cliente ed Interessati • tra Cliente e Fornitore Chiarezza e completezza nel contratto	Rischi dalla presenza di molti Fornitori/Subfornitori Misure tecniche/organizzative e obbligazioni contrattuali	Necessaria certezza nelle operazioni Misure tecniche/organizzative e obbligazioni contrattuali

Tutele contrattuali, trasferimenti di dati all'estero
•Necessario stabilire un contratto tra Cliente e Fornitore •Trasferimento di dati verso paesi extra EEA: •In generale non applicabili i casi di esenzione previsti dalla 95/46/EC •Safe Harbour per i fornitori U.S.A. (comunque per i servizi cloud è opportuno assessment da terza parte) • in generale da preferire le clausole contrattuali standard stabilite dalla UE (es. 2010/87/UE) e/o Binding Corporate Rules

Misure tecnico-organizzative:	
Disponibilità dei dati:	Back-up dei dati e procedure di ripristino /Ridondanza di base dati Adeguate caratteristiche del servizio Internet utilizzato
Integrità dei dati:	Intrusion Detection/prevention Systems, Meccanismi di autentificazione crittografica
Riservatezza dei dati:	Dati crittografati sia in "transito" sulla rete sia quando "residenti" sui server Meccanismi di strong authentication per gli utenti (*)
Trasparenza:	Chiarezza e completezza nel contratto
Trattamenti limitati alle finalità consentite	Governance nella distribuzione e nel controllo dei diritti di accesso ai dati personali (*) e Relative misure tecniche
Corrispondere alle richieste di Esercizio dei diritti:	Obligazioni contrattuali che assicurino al Cliente il supporto del Fornitore (e Subfornitori)
Portabilità dei dati (compatibilità con altri Fornitori-Sistemi)	Verifiche precontrattuali e Obligazioni contrattuali che assicurino la portabilità al termine del Contratto con il Fornitore (quale ne sia il motivo)
Accountability: *In ambito Information Technology: capacità di stabilire cosa è stato fatto e come in un determinato tempo* *In ambito protezione dati: la capacità di dimostrare che sono stati prese le appropriate misure ai fini della conformità alla normativa*	Sono richieste misure tecnico-organizzative per dimostrare l'esistenza di una privacy-security Policy e la sua effettiva implementazione, incluse eventuali certificazioni emesse da terze parti. Necessarie apposite obligazioni contrattuali E' essenziale per consentire al Cliente di corrispondere alle richieste delle autorità competenti (DPA) previste dalla legge *(ad esempio per il caso di "violazione dei dati personali" nei servizi di comunicazione elettronica accessibili al pubblico, introdotto in Italia dal D.Lgs 69/12)*

da: diritto.it

Riassunto Opinion 05/2012 Art.29 WP

WP 29 Opinion 5/12: riepilogo dei principali aspetti del contesto normativo e delle misure individuate

Contesto legislativo EU per la protezione dei dati:	
95/46/EC	2002/58/EC

Legge applicabile:

quella del paese(i) ove il Cliente/Titolare è stabilito

Rapporto Cliente-Fornitore-Subfornitori

Essenziale stabilire:
- la ripartizione delle responsabilità per la conformità alla legge
- come consentire in pratica l'esercizio dei diritti degli Interessati

Principi basilari

Trasparenza	Trattamenti limitati alle finalità consentite	Conservazione dati/cancellazione dei dati
• tra Cliente ed Interessati • tra Cliente e Fornitore Chiarezza e completezza nel contratto	Rischi dalla presenza di molti Fornitori/Subfornitori Misure tecniche/organizzative e obbligazioni contrattuali	Necessaria certezza nelle operazioni Misure tecniche/organizzative e obbligazioni contrattuali

Tutele contrattuali, trasferimenti di dati all'estero

- Necessario stabilire un contratto tra Cliente e Fornitore
- Trasferimento di dati verso paesi extra EEA:
  - In generale non applicabili i casi di esenzione previsti dalla 95/46/EC
  - Safe Harbour per i fornitori U.S.A. (comunque per i servizi cloud è opportuno assessment da terza parte)
  - in generale da preferire le clausole contrattuali standard stabilite dalla UE (es. 2010/87/UE) e/o Binding Corporate Rules

Misure tecnico-organizzative:	
Disponibilità dei dati:	Back-up dei dati e procedure di ripristino /Ridondanza di base dati Adeguate caratteristiche del servizio Internet utilizzato
Integrità dei dati:	Intrusion Detection/prevention Systems, Meccanismi di autentificazione crittografica
Riservatezza dei dati:	Dati crittografati sia in "transito" sulla rete sia quando "residenti" sui server Meccanismi di strong authentication per gli utenti (*)
Trasparenza:	Chiarezza e completezza nel contratto
Trattamenti limitati alle finalità consentite	Governance nella distribuzione e nel controllo dei diritti di accesso ai dati personali (*) e Relative misure tecniche
Corrispondere alle richieste di Esercizio dei diritti:	Obligazioni contrattuali che assicurino al Cliente il supporto del Fornitore (e Subfornitori)
Portabilità dei dati (compatibilità con altri Fornitori-Sistemi)	Verifiche precontrattuali e Obligazioni contrattuali che assicurino la portabilità al termine del Contratto con il Fornitore (quale ne sia il motivo)
Accountability: *In ambito Information Technology capacità di stabilire cosa è stato fatto e come in un determinato tempo* *In ambito protezione dati la capacità di dimostrare che sono stati prese le appropriate misure ai fini della conformità alla normativa*	Sono richieste misure tecnico-organizzative per dimostrare l'esistenza di una privacy-security Policy e la sua effettiva implementazione, incluse eventuali certificazioni emesse da terze parti. Necessarie apposite obligazioni contrattuali E' essenziale per consentire al Cliente di corrispondere alle richieste delle autorità competenti (DPA) previste dalla legge *(ad esempio per il caso di "violazione dei dati personali" nei servizi di comunicazione elettronica accessibili al pubblico, introdotto in Italia dal D.Lgs 69/12)*

(*) presso il Fornitore, i Subfornitori, ..ed il Cliente

da: diritto.it

Aspetti Legali specifici relativi alla Protezione dei dati in generale:

- Quale legge nazionale si deve applicare ?
- Quale insieme di misure di sicurezza deve essere applicato ?
- E' legale trasferire Dati Personali a paesi non-EU ?
- Noi cittadini (cui si riferiscono I dati personli) abbiamo diritti relativamente al controllo dell' utilizzo dei nostri dati ?
- Un Cloud Provider è responsabile legalmente di come gestisce i nostri dati personali ?

Quale legge si deve applicare ?

- Primo punto: Chi è il Controllore dei Dati (Data Controller)?
- Secondo punto: ha sede legale all'interno dell' UE ?
- *La definizione di Sede data da* ***Art. 29 Working Party***
- Terzo Punto : utilizza delle infrastrutture/server situate nell' UE?
- Quello che in definitiva conta è la locazione dei ruoli : Controller e Processor dei dati

Quali sono le norme di sicurezza da applicare ?

L' Articolo 17(3) della Direttiva 95/46/EC stabilisce che sia

- **La sede del processatore dei dati** (Processor's Establishment)

A determinare **quale normativa nazionale** si debba applicare

Trasferimento di dati personali verso paesi non UE

- **OK** verso paesi con livello adeguato di protezione dei dati personali (comprese le organizzazioni che fanno parte del Safe Harbor)

Oppure – Altre possibilità:

- Consenso(o simile, come previsto da art. 26(1) Dir 95/46/EC)
- Contratto (con il destinatario dei dati)
  - Contratto ad hoc
  - Clausole standard
- Norme vincolanti di impresa

I diritti del cittadino cui si riferiscono i Dati Personali (*«Data Subject»*)

- Diritto di accesso ai propri dati personali
- Diritto di rettifica
- Diritto al cancellamento/blocco
- Diritto di obiettare

I Diritti che verranno con la nuova normativa:

- Diritto alla portabilità dei dati da un provider all'altro
- Diritto ad essere informato su ogni violazione dei Dati Personali
- Diritto ad essere completamente dimenticato per sempre
- …

Responsabilità legali del Controllore dei Dati *(«Controller»)*

Il Controllore **deve:**

- Implementare tutte le misure necessarie a tutela dei dati personali
- Assicurare un livello di sicurezza appropriato a seconda dei rischi
- Identificare e scegliere un processatore dei dati (*Data Processor*) che dia adeguate garanzie

Il Controllore **è completamente perseguibile** in termini di legge relativamente al rispetto di queste norme.

Art. 23 Dir. 95/46/EC:

- Ogni persona che è stata danneggiata a causa di processamento dati illegale **ha diritto a ricevere rimborso dal controllore dei dati** per il danno ricevuto.

Responsabilità del Controllore dei Dati

- Art. 29 WP - opinion no. 3/2010

Il controllore dei dati deve:

  - Mettere in piedi efficaci misure di protezione/sicurezza
  - Dimostrarlo alle Autorità di Protezione dei Dati Personali

- Art. 29 WP - opinion no. 5/2012

Il controllore dei dati deve:

  - Dimostrare di aver agito in maniera da implementare I principi di protezione dei dati

- Regulation (GDPR proposal - EU Communication 2012 (11)) Article 22

Protezione della proprietà intellettuale ed altri *assets*

- Un contratto chiaro e solido
- SLAs (PLAs)
- Controllo diretto sul cloud provider (e.s. pannello di controllo)
- Log di accesso ai dati
- Audit di una terza parte indipendente
- Misure efficaci contro il vendor lock-in
- ...

Cambiamenti normativi in vista ?

La prossima normativa sulla protezione dei dati personali

- Un unico testo normativo legale al posto di 27 testi normativi distinti (uno per paese UE)
- La cittadinanza Europea come elemento legislativo da considerare
- Una definizione aggiornata e più attuale, matura di
  - Trasparenza
  - Accountability (Tracciabilità)
  - Diritti del cittadino (Data Subject), ...

Molto bolle nella pentola dell'UE…

- Da fine gennaio 2012 la Commissione sta proponendo una riforma sostanziosa della normativa EU relativa alla protezione dei dati
  - Si vuole modernizzare la normativa del 1995

- Un **unico insieme di norme** per la protezione dei dati sarà in vigore **in tutta l'UE**
  - Semplificazione legislativa e procedurale
  - Nuove, più aggiornate definizioni di trasparenza, tracciabilità e riportistica, diritti dei cittadini relativamente ai loro dati personali……
  - Si terrà conto anche della cittadinanza EU…

La normativa EU unificata che verrà…

- Introduzione del **Diritto all'Oblio**
  - Se non si vuole più consentire trattamento, i dati verranno eliminati
- Consenso al trattamento dei dati **sempre esplicito**
- **Più facile accedere** ai propri dati
- **Portabilità dei dati** da un provider all'altro
- Le imprese dovranno fare riferimento ad **una sola Autorità Nazionale per la protezione dei dati personali**
  - Quella del paese dove hanno la sede principale
- Si avrà **diritto di rivolgersi all'Autorità del proprio paese** anche quando i dati personali sono trattati in un altro paese
- Le norme EU si applicheranno **anche alle imprese che non hanno sede nell'UE**, ma che offrono prodotti o servizi nell'UE o monitorano il comportamento online dei cittadini
- Chi tratta i dati personali avrà in generale **più responsabilità e doveri**
- Saranno **eliminati oneri amministrativi superflui**, come l'obbligo di notifica per imprese che trattano i dati personali
- Sarà **rafforzato il ruolo delle Autorità nazionali** di protezione dei dati per migliorare applicazione delle norme EU a livello nazionale

Le Raccomandazioni del Garante per la Privacy

- Ponderare prioritariamente rischi e benefici dei servizi offerti
- Effettuare una verifica in ordine all'affidabilità del fornitore
- Privilegiare i servizi che favoriscono la portabilità dei dati
- Assicurarsi la disponibilità dei dati in caso di necessità
- Selezionare i dati da inserire nella cloud
- Non perdere di vista i dati
- Informarsi su dove risiederanno, concretamente, i dati
- Prestare molta attenzione alle clausole contrattuali
- Verificare le politiche di persistenza dei dati legate alla loro conservazione
- Esigere e adottare opportune cautele per tutelare la confidenzialità dei dati
- Formare adeguatamente il personale