Percorso integrato
Regolamento europeo per la protezione dei dati (GDPR)

Regolamento Europeo sulla Protezione dei Dati: la nuova normativa in materia di protezione dei dati e gli impatti sulle procedure e sull'organizzazione

Cagliari - 5 aprile 2018
ore 9.30 - 13.30

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

- L'informativa;
- Mezzi di ricorso, responsabilità e sanzioni;
- Trasferimenti transfrontalieri;
- Q&A

Informativa

PRIMA CHE IO SCRIVA IL MIO NOME SULLA LAVAGNA HO BISOGNO DI SAPERE IN CHE MODO SARANNO UTILIZZATI QUESTI DATI PERSONALI

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

Art. 14 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

Art. 15 - Diritto di accesso dell'interessato

Considerando 39: il principio di Trasparenza

Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto.

Dovrebbero essere trasparenti per le persone fisiche le **modalità** con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la **misura** in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che **le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.**

Considerando 39: il principio di Trasparenza

Tale principio riguarda, in particolare, l'informazione degli interessati sull'**identità del titolare** del trattamento e sulle **finalità del trattamento** e **ulteriori informazioni** per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.

Considerando 39: il principio di Trasparenza

È opportuno che le persone fisiche siano **sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti** relativi al trattamento dei dati personali, nonché alle **modalità di esercizio dei loro diritti** relativi a tale trattamento. In particolare, **le finalità specifiche** del trattamento dei dati personali **dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali**.

Considerando 61

L'interessato **dovrebbe ricevere le informazioni** relative al trattamento di dati personali che lo riguardano **al momento della raccolta presso l'interessato o**, se i dati sono ottenuti da altra fonte, **entro un termine ragionevole**, in funzione delle circostanze del caso.

Considerando 62

Per contro, **non è necessario** imporre l'obbligo di **fornire l'informazione**

- **se l'interessato dispone già dell'informazione**,
- **se la registrazione o la comunicazione dei dati personali sono previste per legge** o
- se **informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato**.
- Quest'ultima eventualità potrebbe verificarsi, ad esempio, nei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi si può tener conto del numero di interessati, dell'antichità dei dati e di eventuali garanzie adeguate in essere.

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) **l'identità e i dati di contatto del titolare** del trattamento e, ove applicabile, del suo rappresentante;

b) i **dati di contatto del responsabile della protezione dei dati**, ove applicabile;

c) le **finalità del trattamento** cui sono destinati i dati personali nonché la **base giuridica del trattamento**;

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i **legittimi interessi perseguiti dal titolare del trattamento o da terzi**;

e) gli **eventuali destinatari o le eventuali categorie di destinatari** dei dati personali;

f) ove applicabile, **l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione** o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il **riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili**.

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) **l'esistenza del diritto dell'interessato** di chiedere al titolare del trattamento l'**accesso** ai dati personali e la **rettifica** o la **cancellazione** degli stessi o la **limitazione** del trattamento che lo riguardano o di **opporsi** al loro trattamento, oltre al diritto alla **portabilità dei dati**;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del **diritto di revocare il consenso in qualsiasi momento** senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il **diritto di proporre reclamo** a un'autorità di controllo;

e) **se la comunicazione di dati personali è un obbligo legale o contrattuale** oppure un requisito necessario per la conclusione di un contratto, e **se l'interessato ha l'obbligo di fornire i dati personali** nonché le **possibili conseguenze della mancata comunicazione** di tali dati;

f) **l'esistenza di un processo decisionale automatizzato**, compresa la **profilazione** di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla **logica utilizzata**, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

3. Qualora il titolare del trattamento intenda trattare **ulteriormente** i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'**interessato dispone già delle informazioni.**

In cosa resta uguale ad oggi?

- **Se i dati sono raccolti presso l'interessato l'informativa deve precedere il trattamento**
- **Se i dati non sono raccolti presso l'interessato l'informativa deve indicare le categorie dei dati personali oggetto di trattamento**
- **Il Titolare deve indicare i propri dati e quelli dell'eventuale rappresentante nel territorio italiano**
- **Deve indicare le finalità del trattamento**
- **Deve indicare i diritti dell'interessato**
- **Deve indicare l'eventuale responsabile del trattamento (data processor)**
- **Deve indicare i destinatari dei dati**

Come cambia l'informativa nel GDPR?

Contenuti

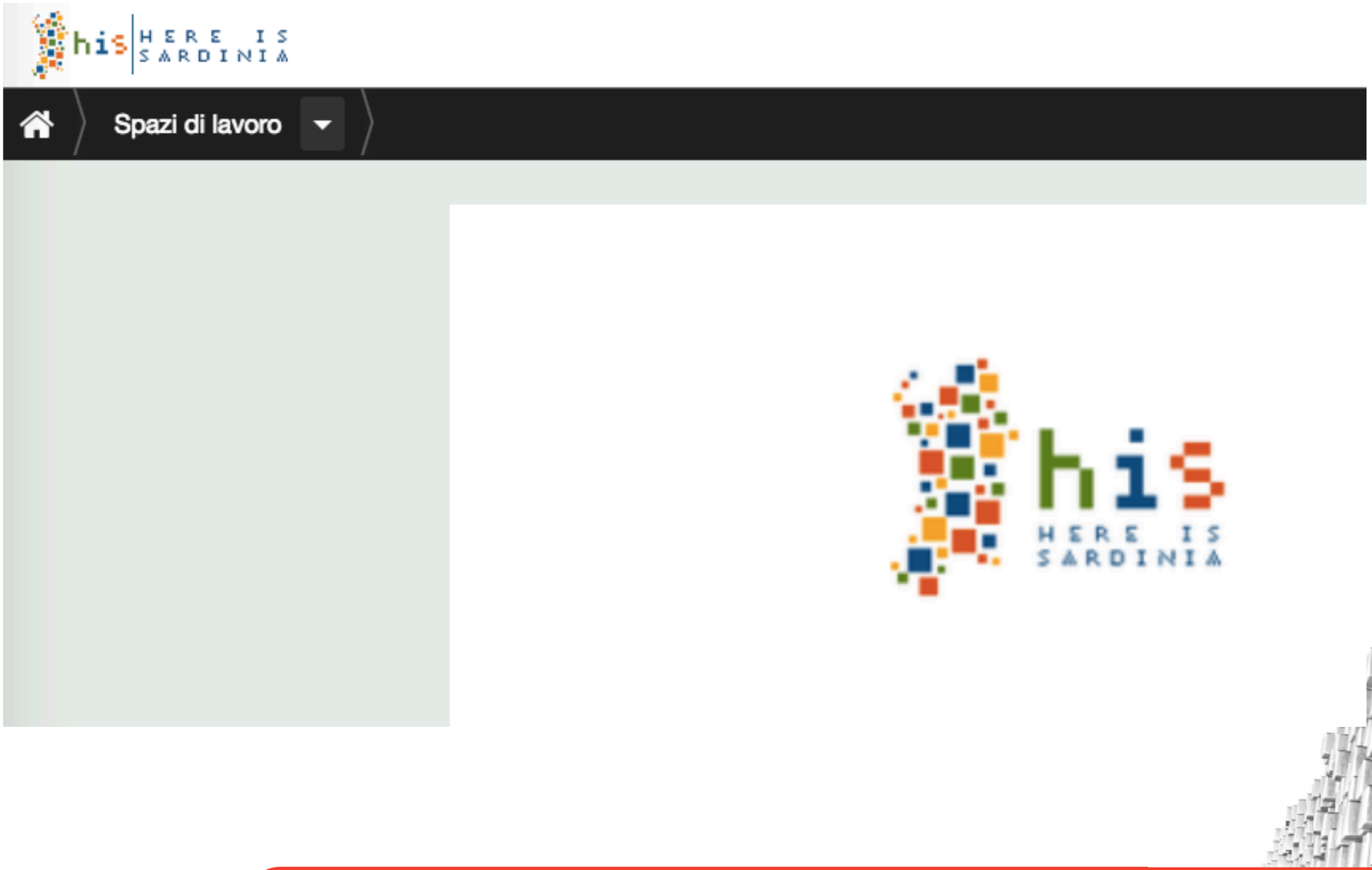
- **Dati di contatto del Data Protection Officer**
- **Base giuridica del trattamento**
- **Interesse legittimo al trattamento** (non applicabile alle PA)
- **Indicazione se sia previsto il trasferimento di dati in Paesi terzi**
  - **in caso affermativo: attraverso quali strumenti**
- **Periodo di conservazione dei dati**
  - **Nel caso non possa indicarsi il periodo preciso si dovrà, almeno, indicare i criteri stabiliti per stabilire la durata della conservazione**
- **Il diritto di presentare reclamo all'Autorità di controllo**
- **Si deve specificare se il trattamento comporta processi decisionali automatizzati e, nel caso, la logica dei processi decisionali e le possibili conseguenze per l'interessato**

Tempi dell'informativa

- Se i dati non sono raccolti presso gli interessati entro un termine ragionevole dall'ottenimento dei dati personali, ma **al più tardi entro un mese (dalla raccolta);**
- Se i dati non sono raccolti presso l'interessato ma sono destinati alla comunicazione con l'interessato, al più tardi **al momento della prima comunicazione all'interessato;**
- Se i dati non sono raccolti presso l'interessato ma sono destinati alla comunicazione ad altro destinatario, **non oltre la prima comunicazione dei dati personali**.

Forma dell'informativa

- In linea di principio è data **per iscritto e (preferibilmente) in formato elettronico**
- Potranno essere previste delle **icone in combinazione con l'informativa estesa** (le icone sono approvate dalla Commissione europea)
- L'informativa deve essere **concisa, trasparente, intelligibile** (linguaggio chiaro e semplice) **e facilmente accessibile**


HERE IS SARDINIA
Spazi di lavoro
HERE IS SARDINIA

Here is Sardinia

L'applicazione "Here is Sardinia" – disponibile attraverso il PlayStore di Google (per le applicazioni Android) e Apple Store – è un'App creata da SardegnaIT.

Al momento dell'installazione, tale Applicazione richiede i seguenti consensi:

- identità dell'utente (account sul dispositivo, dati profilo),
- posizione (geolocalizzazione del dispositivo),
- foto/elementi multimediali/file (non attiva)
- informazioni sulla connessione Wi-Fi

All'atto della registrazione dell'utente si può optare tra un utilizzo di Facebook o Twitter quali gestori di identità, ovvero attraverso la registrazione tradizionale mediante inserimento di alcuni dati personali (**email, nome, cognome, sesso, data di nascita, città di residenza**). La richiesta di consenso, una volta fornita l'informativa, non è "pre-flaggata".

Informativa HiS. Attenzione a...

- finalità indicate (ad esempio si dice, genericamente, che – per quanto riguarda la comunicazione dei dati degli utenti di HIS a terzi – "potrebbero essere comunicati a soggetti esterni", senza, però, indicare per quali finalità potrebbe sorgere la necessità di tale comunicazione di dati personali.
- luogo del trattamento ("in ogni altro luogo in cui le parti coinvolte nel trattamento siano localizzate")
- inserimento dell'indirizzo dell'utente in una mailing list al fine di ottenere informazioni "anche di natura commerciale e promozionale" (indicare se tale inserimento sia facoltativo o obbligatorio).
- il Titolare del trattamento dei dati personali.
- durata della conservazione,
- base giuridica del trattamento
- indicazione dei contatti del Data Protection Officer
- eventuali flussi extra-UE dei dati personali (Amazon AWS - EU)

Clausola zombie AWS Amazon

57.10 Acceptable Use; Safety-Critical Systems. Your use of the Lumberyard Materials must comply with the AWS Acceptable Use Policy. The Lumberyard Materials are not intended for use with life-critical or safety-critical systems, such as use in operation of medical equipment, automated transportation systems, autonomous vehicles, aircraft or air traffic control, nuclear facilities, manned spacecraft, or military use in connection with live combat.

However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization.

https://aws.amazon.com/it/service-terms/

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;	Sono contitolari del trattamento i seguenti soggetti: RAS, SOGAER, SOGEAL, …
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;	Il Responsabile della protezione dei dati personali può essere contattato mediante <…> all'indirizzo <…>
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;	finalità di osservatorio, accoglienza e promozione turistica. <inserire anche le finalità dei contitolari>
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;	NON PREVISTO PER LE PA
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;	I dati personali possono essere comunicati a <…>

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.	// non vengono trasferiti al di fuori dello SEE
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;	**I DATI VENGONO CONSERVATI PER <$TEMPO>. PER CRITERIO: I DATI VENGONO CONSERVATI PER UN PERIODO DI TRE ANNI DALL'ULTIMO UTILIZZO DELLA APP HiS**
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;	**…**

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;	non riguarda la PA ma solo i partner privati. La revoca del consenso deve, comunque, essere "tracciato" (accountability)
d) il diritto di proporre reclamo a un'autorità di controllo;	
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;	pur in assenza di un obbligo contrattuale o normativo sarà necessario, per il funzionamento dell'App quantomeno la UserID e l'indirizzo email. Le altre informazioni sono facoltative ma sono indispensabili alla personalizzazione dei servizi quali <…> Per le finalità dei contitolari <A, B, C…> la prestazione del consenso è, comunque, facoltativa.

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.	

Mezzi di ricorso, responsabilità e sanzioni

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Strumenti di tutela amm.va e giur.le

- **Tutela in via amministrativa di fronte all'Autorità di controllo riguardo un trattamento in violazione del GDPR**

- **Tutela giurisdizionale di fronte a un provvedimento o decisione dell'autorità di controllo**

- **Tutela giurisdizionale a tutela di un diritto riconosciuto dal GDPR**

Art 77 Diritto di proporre reclamo all'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, ***l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo****, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.*

Art 78 Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo

1. *Fatto salvo ogni altro ricorso amministrativo o extragiudiziale,* ***ogni persona fisica o giuridica*** *ha il diritto di proporre un* ***ricorso giurisdizionale*** *effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.*

2. *Fatto salvo ogni altro ricorso amministrativo o extragiudiziale,* ***ciascun interessato*** *ha il diritto di proporre un* ***ricorso giurisdizionale*** *effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.*

Art 79 Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ***ogni interessato ha il diritto di proporre un ricorso giurisdizionale*** *effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.*

2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

La “vecchia” regolamentazione della responsabilità civile

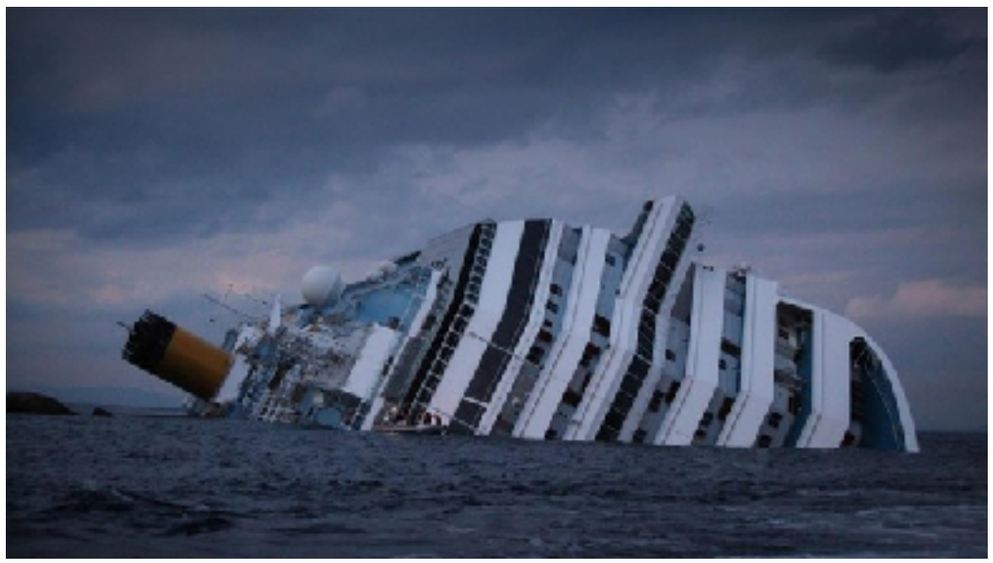
1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 15 Cod. Privacy

Responsabilità civile

Art. 2050 cod. civ.
*Chiunque cagiona danno ad altri nello svolgimento di un'**attività pericolosa,** per sua natura o per la natura dei mezzi adoperati , è tenuto al risarcimento, se non **prova** di avere adottato tutte le misure idonee a evitare il danno*



Attività pericolosissime

Responsabilità civile

Nessun trattamento è escluso
Anche il trattamento di dati personali effettuato da persone fisiche per **fini esclusivamente personali** è espressamente soggetto all'applicabilità della disciplina in tema di responsabilità (oltre che a quella in tema di sicurezza) – art. 5

Responsabilità civile

Soggetto
che ha subito un danno

Prova che si tratti di un'attività pericolosa (non necessaria)

Prova del nesso causale tra il danno e l'attività

Responsabilità civile

Il titolare del trattamento che ha cagionato il danno

Fornisce la prova di aver adottato " tutte le misure idonee"

Non sarà responsabile

Non fornisce la prova di aver adottato " tutte le misure idonee"

Sarà ritenuto responsabile

TECNOLOGIA

18 luglio 2017

Ashley Madison pagherà 12 milioni di dollari a vittime cyber attacco

Il sito dedicato alle relazioni extraconiugali Ashley Madison ha annunciato che risarcirà le vittime del cyber-attacco del 2015 (foto di archivio - Getty Images)

La compagnia Ruby Life Inc risarcirà gli utenti americani del sito dedicato alle relazioni extraconiugali. L'accordo è stato raggiunto dopo la class action

Le cifre del risarcimento

Secondo quanto dichiarato dall'azienda chi ha subito una perdita consistente potrà aspirare al massimo del risarcimento, ovvero 3.500 dollari. Questo patteggiamento è stato deciso per evitare future cause singole tra le vittime e l'azienda. L'accusa principale mossa all'azienda dopo l'attacco del 2015 è che la sicurezza dei dati fosse inadeguata. Secondo le stime del Wall Street Journal, gli utenti che potrebbero accedere all'accordo con la Ruby Life Inc. sono 6 milioni. In tal caso, dovendosi spartire 11,8 milioni di dollari, la cifra che spetterebbe loro scenderebbe da 3.500 dollari a soli 2 dollari ciascuno.

Violazione di dati personali e responsabilità civile

Il danno non patrimoniale risarcibile ai sensi dell'art. 15 del d.lgs. 30 giugno 2003, n. 196 (c.d. codice della privacy) non si sottrae alla verifica di "gravità della lesione" (concernente il diritto fondamentale alla protezione dei dati personali, quale intimamente legato ai diritti ed alle libertà indicate dall'art. 2 del codice, convergenti tutti funzionalmente alla tutela piena della persona umana e della sua dignità) e di "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), che, in linea generale, si richiede in applicazione dell'art. 2059 cod. civ. nelle ipotesi di pregiudizio inferto ai diritti inviolabili previsti in Costituzione

Ove l'offesa non superi la **soglia di minima tollerabilità o il danno sia futile**, si può escludere la possibilità di somministrare il risarcimento del danno

Cass., Sez. 3, sent. 16133/2014

Art 82 Diritto al risarcimento e responsabilità

1. ***Chiunque subisca un danno materiale o immateriale*** *causato da una violazione del presente regolamento* ***ha il diritto di ottenere il risarcimento del danno dal titolare*** *del trattamento* ***o dal responsabile*** *del trattamento.*

2. *Un* ***titolare*** *del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un* ***responsabile*** *del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.*

3. ***Il titolare*** *del trattamento* ***o il responsabile*** *del trattamento* ***è esonerato dalla responsabilità****, a norma del paragrafo 2* ***se dimostra che l'evento dannoso non gli è in alcun modo imputabile****.*

differenze titolare-responsabile

TITOLARE → Risponde del danno cagionato da violazione del GDPR

RESPONSABILE → Risponde del danno se ha agito in difformità rispetto alle istruzioni legittime del titolare

Art 82 Diritto al risarcimento e responsabilità

4. Qualora ***più titolari del trattamento o responsabili*** *del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato* **[solidarietà passiva]**

5. Qualora ***un titolare del trattamento o un responsabile del trattamento abbia pagato****, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2* **[regresso]**.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Responsabilità e sanzioni nel GDPR

Art. 83 - condizioni generali sulle sanzioni amministrative pecuniarie

Art. 84 - delega agli Stati membri all'adozione di sanzioni per violazioni non previste dal GDPR

L'art. 83 - Se e in quale misura sanzionare le PA

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ***ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici*** *istituiti in tale Stato membro.*

Comitato europeo per la protezione dei dati

ai sensi dell'articolo 70, paragrafo 1, lettera e), il comitato europeo per la protezione dei dati ha la facoltà di pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento, e l'articolo 70, paragrafo 1, lettera k), specifica che è prevista l'elaborazione di linee guida riguardanti la previsione di sanzioni amministrative pecuniarie

I poteri delle DPA

Le disposizioni di cui all'articolo 58, paragrafo 2, lettere da b) a j), indicano gli strumenti che le autorità di controllo hanno a disposizione per far fronte a un'inadempienza da parte di un titolare del trattamento o responsabile del trattamento:

(B)rivolgere **ammonimenti** al titolare o al responsabile del trattamento
(C)ingiungere al titolare o al responsabile del trattamento di **soddisfare le richieste dell'interessato**;
(D)ingiungere al titolare del trattamento o al responsabile del trattamento di **conformare i trattamenti alle disposizioni del regolamento**, se del caso, in una determinata maniera ed entro un determinato termine;
(E)ingiungere al titolare del trattamento di **comunicare all'interessato una violazione dei dati personali**;
(F)**imporre una limitazione provvisoria o definitiva al trattamento**;
(G)**ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento**;
(H)**revocare la certificazione**;
(I)**infliggere una sanzione amministrativa pecuniaria**;
(J)**ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo** o un'organizzazione internazionale.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

17/IT

WP 253

Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679

Adottate il 3 ottobre 2017

Principi destinati alle DPA (in Italia il Garante)

1. La violazione del regolamento dovrebbe comportare l'imposizione di "**sanzioni equivalenti**"

2. Come tutte le misure correttive scelte dalle autorità di controllo, le sanzioni amministrative pecuniarie dovrebbero essere "**effettive, proporzionate e dissuasive**"

3. L'autorità di controllo competente effettuerà una valutazione "in ogni singolo caso"

4. Un approccio armonizzato alle sanzioni amministrative pecuniarie in materia di protezione dei dati richiede la partecipazione attiva delle autorità di controllo e lo scambio di informazioni tra le stesse

Sanzioni “multilivello”

Le sanzioni amministrative pecuniarie possono essere inflitte in combinazione o in sostituzione delle misure previste dall’art. 58 GDPR

Principi destinati alle DPA (in Italia il Garante)

1. La violazione del regolamento dovrebbe comportare l'imposizione di "**sanzioni equivalenti**"

2. Come tutte le misure correttive scelte dalle autorità di controllo, le sanzioni amministrative pecuniarie dovrebbero essere "**effettive, proporzionate e dissuasive**"

3. L'autorità di controllo competente effettuerà una valutazione "in ogni singolo caso"

4. Un approccio armonizzato alle sanzioni amministrative pecuniarie in materia di protezione dei dati richiede la partecipazione attiva delle autorità di controllo e lo scambio di informazioni tra le stesse

L'art. 83 - concorso di violazioni

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, ***l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.***

L’art. 83 - importo delle sanzioni

4. In conformità del paragrafo 2, ***la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR****, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:*

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

L’art. 83 - importo delle sanzioni

5. In conformità del paragrafo 2, ***la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR****, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:*

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

Criteri di valutazione di cui all'articolo 83

a) la natura, la gravità e la durata della violazione;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

Criteri di valutazione di cui all'articolo 83

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Q&A

Domanda 1

Immissione volontaria di dati da parte di operatori economici su sistemi informativi dell'assessorato: **l'immissione avviene, previa autenticazione, per diverse finalità** (inserimento anagrafica commerciale, partecipazione a progetti, iscrizione a gruppi, etc) e può in alcuni casi ricomprendere dati personali (es: numero cellulare guida turistica); **occorre comunque informativa che dettagli chi è il DPO, a quali fini e dove sono conservati i dati, etc?**

Risposta… secca

Si. L'informativa deve precedere il trattamento

Domanda 2

2) Quando si concretizzano le condizioni di contitolarità del dato, quali sono i presupposti?

Risposta...

Esaminiamo qualche provvedimento del Garante…

Risposta...

È lecito il trattamento dei dati effettuato dal Comune, in "contitolarità" con Questura e Comando dei Carabinieri, mediante l'installazione nel centro cittadino di un sistema di videosorveglianza ove non emergano profili di illiceità del trattamento e risultino rispettati i limiti fissati dal provvedimento di carattere generale emesso dal Garante in materia del 29/11/2000 (nel caso di specie il Garante ha rilevato che non erano state attivate alcune funzioni delle apparecchiature di ripresa particolarmente invasive quali i sistemi di registrazione delle conversazioni, di illuminazione ad infrarossi e di riconoscimento biometrico facciale).

- Garante 30 dicembre 2002 [doc. web n. 1067284]

Risposta...

È lecito il trattamento dei dati effettuato dal Comune, in "contitolarità" con Questura e Comando dei Carabinieri, mediante l'installazione nel centro cittadino di un sistema di videosorveglianza, ove non emergano profili di illiceità del trattamento e risultino rispettati i limiti fissati dal provvedimento di carattere generale emesso dal Garante in materia del 29 novembre 2000 (nel caso di specie il Garante ha rilevato che non erano state attivate alcune funzioni delle apparecchiature di ripresa particolarmente invasive quali i sistemi di registrazione delle conversazioni, di illuminazione ad infrarossi e di riconoscimento biometrico facciale).

- Garante 9 gennaio 2003 [doc. web n. 1067775]
- Garante 9 gennaio 2003 [doc. web n. 1067813]

Domanda 3

Trattamento transfrontaliero: ci avvaliamo di SAAS che possono avere carattere transfrontaliero. È necessario acquisire dai relativi provider riscontro formale del fatto che i servizi erogati abbiano o meno tale carattere? e in tal caso, è sufficiente una loro attestazione formale della conformità al GDPR?

Trasferimenti transfrontalieri

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali e nuove tecnologie

Considerando 6 GDPR

“La tecnologia...dovrebbe facilitare ancora di più la libera circolazione dei dati personali...e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali”

Nel GDPR (Capo V)

Art. 44 - Principio generale per il trasferimento

Art. 45 - Trasferimento sulla base di una decisione di adeguatezza

Art. 46 - Trasferimento soggetto a garanzie adeguate

Art. 47 - Norme vincolanti d'impresa

Art. 48- Trasferimento o comunicazione non autorizzati dal diritto dell'Unione

Art. 49 - Deroghe in specifiche situazioni

Art. 50 - Cooperazione internazionale per la protezione dei dati personali

Il bilanciamento tra due interessi contrapposti...

Da un lato: consolidare le garanzie degli interessati i cui dati vengono trasferiti

VS

Dall'altro: soddisfare le ragioni economiche del mondo digitale e incoraggiare la liberalizzazione dei flussi transfontalieri

Principio generale per il trasferimento
Art. 44 GDPR

CHI: titolare del trattamento e responsabile del trattamento

COME: rispetto delle condizioni del GDPR (*conditio sine qua non*)

FINALITÀ: assicurare il livello di protezione (C101-102)

Principio generale ed eccezioni per poter effettuare trasferimenti transnazionali

Regola:

adeguatezza della tutela

Eccezioni:

artt. 48 e 49 GDPR

Trasferimento sulla base di una decisione di adeguatezza
Art. 45 GDPR

Il TRASFERIMENTO E' AMMESSO quando

la Commissione valuta, attraverso una attestazione formale, l'adeguatezza della protezione dei dati personali nel Paese terzo o nell'organizzazione internazionale e decide che questi ultimi garantiscono un livello di protezione adeguato

Quando manca una decisione di adeguatezza...

Clausole contrattuali tipo

(standard contractual clauses/model clauses/SCC)

- **già previste nell'art. 26, 4° comma Direttiva 95/46/CE**
  (strumento derogatorio al generale divieto di trasferimento in Paesi terzi che non garantiscono un livello di tutela adeguato)
- **art. 46 GDPR**

Che cosa sono

<u>testo contrattuale standard</u> che prevede la sottoscrizione da parte dei soggetti fra cui avviene il flusso di dati, con il quale si impegnano a garantire un adeguato livello di protezione dei dati trasferiti

Chi le predispone (GDPR)

- **la Commissione europea**

oppure

- **Autorità nazionale di controllo + approvazione della Commissione europea**

(art. 46, par. 2, lett. c e d)

Le decisioni della Commissione sulle *standard contractual clauses*

Nel vigore della Direttiva 95/46/CE la Commissione ha adottato quattro decisioni con le quali ha definito gli assetti delle clausole contrattuali standard utilizzabili

Termine di validità

art. 46, par. 5 GDPR

“fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione”

Novità introdotte dal GDPR

Le clausole contrattuali possono essere utilizzate non solo se i soggetti dello scambio sono due titolari o un titolare e un responsabile del trattamento <u>ma anche quando i soggetti siano due responsabili del trattamento</u>

Allo stato la Commissione sta cooperando con il Gruppo di lavoro ex art. 29 per la formulazione di clausole di tale tipo

ed ancora...

le parti possono ampliare il contenuto delle *standard contractual clauses*, così il C109 *"...includere tali clausole in tipo in un contratto più ampio...aggiungere altre clausole o garanzie supplementari"*

purchè

"non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate dalla Commissione o da una autorità di controllo o ledano i diritti o le libertà fondamentali degli interessati"

Se le parti vogliono stipulare clausole contrattuali diverse da quelle standard...le "*clausole autorizzate*"

art. 46, par. 3 lett. a)

<u>consentito</u>

ma

è necessaria una <u>specifica approvazione</u> della Autorità Garante nazionale

(C108 "*clausole contrattuali autorizzate da un'autorità di controllo*")

L’art. 28 del GDPR

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest’ultimo ricorre unicamente a responsabili del trattamento che presentino **garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell’interessato**.

2. Il **responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale**, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l’aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l’opportunità di opporsi a tali modifiche.

L’art. 28 del GDPR

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell’Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la **materia disciplinata** e la **durata del trattamento**, la **natura e la finalità del trattamento**, il **tipo di dati personali e le categorie di interessati**, gli **obblighi e i diritti del titolare del trattamento**.

L’art. 28 del GDPR

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un’organizzazione internazionale, salvo che lo richieda il diritto dell’Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell’articolo 32;

L'art. 28 del GDPR

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

L'art. 28 del GDPR

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

L’art. 28 del GDPR

Regolamentazione dei rapporti tra responsabile e subresponsabile e “responsabilità del responsabile” nei confronti del titolare per gli inadempimenti del subresponsabile

Codici di condotta e meccanismi di certificazione come elemento per dimostrare la sussistenza delle garanzie

Future clausole contrattuali tipo (da parte della Commissione o delle Autorità di controllo)

Contratto anche in “formato elettronico”

Il responsabile che violi il regolamento, determinando modalità e finalità del trattamento è considerato titolare (fatti salvi gli articoli 82, 83 e 84)

Identificazione indiretta della persona e dei test di deanonimizzazione

ARTICLE 29 DATA PROTECTION WORKING PARTY

0829/14/EN
WP216

Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

In this Opinion, the WP analyses the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them.

data controllers should focus on the concrete means that would be necessary to reverse the anonymisation technique, notably regarding the cost and the know-how needed to implement those means and the assessment of their likelihood and severity.

It should be noted that the identification risk may increase over time and depends also on the development of information and communication technology.

When considering using anonymisation techniques, data controllers have to take into account the following risks

- A specific pitfall is to consider pseudonymised data to be equivalent to anonymised data.

- A second mistake is to consider that properly anonymised data deprive individuals of whatever safeguards – first and foremost, because other pieces of legislation may apply to the use of these data

- A third negligence would also result from not considering the impact on individuals, under certain circumstances, by properly anonymised data, especially in the case of profiling

Different anonymisation practices and techniques exist with variable degrees of robustness.

techniques of de-identification and anonymisation are the subject of ongoing research and such research has shown consistently that no technique is devoid of shortcomings per se

Conclusioni

In many cases, an **anonymised dataset can still present residual risk** to data subjects. Indeed, even when it is no longer possible to precisely retrieve the record of an individual, it may remain possible to glean information about that individual with the help of other sources of information that are available (publicly or not). It has to be highlighted that beyond the direct impact on data subjects produced by the consequences of a poor anonymisation process (annoyance, time consumption and feeling of lost control by being included in a cluster without awareness or prior consent), other indirect side effects of poor anonymisation may occur whenever a data subject is included in a target erroneously by some attacker, as a consequence of processing anonymised data - especially if the attacker's intents are malicious. Therefore the Working Party stresses that **anonymisation techniques can provide privacy guarantees, but only if their application is engineered appropriately** – which means that the prerequisites (context) and the objective(s) of the anonymisation process must be clearly set out in order to achieve the targeted anonymisation level.

Grazie

per l'attenzione

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi