Conservazione dati personali e dati in cloud

A cura di:

Avv. Cristiana Luciani

Funzionario GPDP

Webinar – 19 novembre 2021

TaxLawPlanet™ *Webinar*

Principio di conservazione

Art. 5, lett. e) RGPD

- I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

GDPR - accountability

- Principio più innovativo del GDPR
- Deriva dalla cultura anglosassone tradotto (impropriamente) in «Responsabilizzazione»: responsabilità, affidabilità, obbligo di rendicontazione
- Pilastro del nuovo impianto normativo
- Il protagonista diventa il titolare del trattamento
- Adotta tutte le misure tecniche ed organizzative adeguate

GDPR - accountability

- Registro dei trattamenti
- Ha una visione completa ed integrata, informatica, giuridica ed organizzativa e piena consapevolezza di tutto ciò che avviene nella struttura
- E' in grado di dimostrare che il trattamento dei dati personali degli interessati è effettuato nel rispetto del GDPR

Titolare del trattamento

- Definisce ogni tipologia di trattamento nelle sue linee essenziali (anche relativa alle modalità e ai tempi di conservazione)
- Acquisisce consapevolezza delle attività di trattamento necessarie per svolgere il proprio lavoro
- Rende subito evidente all'Autorità di controllo quali siano le linee fondamentali dei trattamenti effettuati dall'azienda

Rischi

- Una conservazione «non corretta» comporta gravi rischi
- Es. conservazione green pass da parte del datore di lavoro (d.l. 127/2021)
  - esenzione dai controlli
  - possibile elusione delle finalità di sanità pubblica (vana la possibilità di accertare l'eventuale positività sopravvenuta dell'intestatario del green pass)

Rischi

- Dalla data di scadenza della certificazione, infatti, è agevolmente desumibile quale sia il presupposto per il rilascio della stessa, sicché deve intendersi violato il diritto alla riservatezza del singolo soggetto.
- Contrasto con il Considerando 48 del Reg. 2021/953, a mente del quale il certificato utilizzato per scopi non medici non può essere conservato

- Consenso del lavoratore viziato dall'asimmetria tipica del rapporto lavorativo

Conservazione dei dati di traffico

- Data retention – direttiva 2006/24/CE
  - Attacchi terroristici
  - Conservazione e accesso delle autorità pubbliche per finalità di sicurezza ai dati di traffico delle comunicazioni
  - Bilanciamento tra finalità di sicurezza nel settore della prevenzione e contrasto del terrorismo
  - Necessità e stretta proporzionalità della raccolta
  - Evitare la sorveglianza di massa

Data retention – direttiva 2006/24/CE

- Sentenza Digital Rights Ireland Corte di Giustizia 8/4/2014
  - La direttiva è illegittima per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza (direttiva 2002/58 si è riespansa a seguito dell'invalidazione della 2006/24 ad opera della sentenza Digital Rights)
  - le misure di conservazione dei dati applicabili in via indifferenziata e generalizzata "all´insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell´obiettivo della lotta contro i reati gravi";
  - omesso di prevedere alcun criterio oggettivo che limiti l´accesso a tali dati per sole esigenze di accertamento di reati "sufficientemente gravi da giustificare una simile ingerenza", ben oltre - dunque - il generico rinvio ai reati gravi definiti da ciascuno Stato membro;

Data retention – direttiva 2006/24/CE

- omesso di sancire i presupposti sostanziali e procedurali ai quali subordinare l´accesso, da parte delle competenti autorità nazionali, ai dati in esame, in particolare non richiedendo in ogni caso il previo controllo dell´autorità giudiziaria o di un´autorità amministrativa indipendente;
- omesso di prevedere criteri necessari a differenziare la durata della conservazione dei dati, limitandosi a stabilirne i soli termini minimi e massimi;
- omesso di imporre che i dati così acquisiti siano conservati nel (solo) territorio della Ue.

Data retention – direttiva 2006/24/CE

- Sentenza Corte di giustizia dell'Unione europea del 2/3/2021
  - Segnalazione del GPDP(2/8/21) al Parlamento circa l'opportunità della riforma della disciplina della conservazione dei dati di traffico telefonico e telematico a fini di giustizia (art. 132 d.lgs. 30 giugno 2003, n. 196 e s.m.i.; art. 24 l. 20 novembre 2017, n. 167)
  - La carenza di proporzionalità della disciplina interna è risultata poi accentuata dalla novella di cui alla legge 167 del 2017, che ha esteso a sei anni (72 mesi) il termine massimo di conservazione dei tabulati
  - riforma della disciplina della data retention, tale da differenziare condizioni, limiti e termini di conservazione dei dati di traffico telefonico e telematico in ragione della particolare gravità del reato per cui si proceda, comunque entro periodi massimi compatibili con il richiamato principio di proporzionalità, come interpretato dalla Corte di giustizia dell'Unione europea

Osservazioni sulla conservazione del traffico telefonico

- L'avvocato generale della Corte di Giustizia ricorda che la conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione relativi alle comunicazioni elettroniche è autorizzata solo in caso di grave minaccia alla sicurezza nazionale

Conclusioni dell'Avvocato generale nelle cause riunite C-793/19 e C-794/19, nella causa C-140/20 e nelle cause riunite C-339/20 e C-397/20 – 18 novembre 2021

D.L.30/09/2021 n.132/2021

- Convertito in legge
- Innova la disciplina dell'acquisizione – ai fini dell'utilizzo in procedimenti penali– dei tabulati telefonici e telematici
- i presupposti di straordinaria necessità e urgenza ex art. 77 Cost, sottesi al decreto-legge, sono ravvisati nell'esigenza di adeguare la normativa in materia ai principi sanciti dalla sentenza CGUE del 2 marzo scorso, C-746/18
- Il valore conferito dalla disciplina italiana (art. 132 d.lgs. 196 del 2003) alla gravità dei reati (quale requisito idoneo a regolare la distanza cronologica dell'acquisizione e non la sua ammissibilità) non era del tutto in linea con le affermazioni della Corte
- Giurisprudenza consolidata, che sin dal 2014 con sent. Digital Rights e poi da ultimo con sent. 2/3/2021, aveva affermato come spettasse "al giudice o a un'autorità amministrativa indipendente" l'autorizzazione all'accesso ai dati

D.L.30/09/2021 n.132/2021

- In linea con le indicazioni contenute nella segnalazione del GPDP al Parlamento, il decreto-legge dispone, all'articolo 1, la piena giurisdizionalizzazione della procedura di acquisizione e la selezione dell'ambito oggettivo di applicazione della procedura stessa, esperibile solo nell'ambito dei procedimenti per reati connotati da una determinata gravità, in presenza di sufficienti indizi e della rilevanza dell'acquisizione ai fini dell'accertamento dei fatti .
- ai fini della definizione della gravità dei reati per i quali si ammette l'acquisizione dei tabulati, pare ragionevole la previsione della comminatoria edittale massima di tre anni, combinata con i parametri, da apprezzare in concreto, della sufficienza indiziaria e della rilevanza investigativa del dato da acquisire e con la previsione ad hoc dei reati di minaccia e molestie telefoniche
- inutilizzabilità dei dati acquisiti in violazione delle regole di acquisizione (ordinaria e d'urgenza)

Art.1 D.L.30/09/2021 n.132/2021

All'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) il comma 3 e' sostituito dal seguente:

«3. Entro il termine di conservazione imposto dalla legge, se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti ai fini della prosecuzione delle indagini, i dati sono acquisiti presso il fornitore con decreto motivato del giudice su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private.»;

b) dopo il comma 3 sono inseriti i seguenti:

«3-bis. Quando ricorrono ragioni di urgenza e vi e' fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati

Art.1 D.L.30/09/2021 n.132/2021

b) dopo il comma 3 sono inseriti i seguenti:

«3-bis. Quando ricorrono ragioni di urgenza e vi e' fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che e' comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non e' convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati.

3-ter. Rispetto ai dati conservati per le finalita' indicate al comma 1 i diritti di cui agli articoli da 12 a 22 del Regolamento possono essere esercitati con le modalita' di cui all'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo.»

CLOUD

- Progressiva digitalizzazione
  - Flessibilità del dimensionamento delle risorse informatiche
  - Passaggio ad un modello «*as a service*»
- Si concretizza nella disponibilità di risorse informatiche accessibili da remoto
- È la categoria di servizi di comunicazione di:
  - Audio
  - Video
  - Altri media
- Senza il coinvolgimento dell'operatore di rete nel controllo o distribuzione del contenuto (chat, chiamate in video o in audio, servizi di video streaming)
- I servizi sono forniti sotto forma di applicazioni che eseguono il servizio di accesso ad Internet

CLOUD

PRIVATE

- Infrastruttura informatica pensata per soddisfare specifiche esigenze di una singola organizzazione
- Personalizzazione del servizio offerto dal provider

PUBLIC

- Infrastruttura è proprietà del fornitore del servizio
- Viene messa a disposizione di una pluralità di destinatari
- No unità di memorizzazione dedicati ad uno specifico utente
- Dati provenienti dai diversi utilizzatori archiviati secondo criteri di spazio e di gestione efficiente delle memorie

Over The Top

- È la categoria di servizi di comunicazione di:
  - Audio
  - Video
  - Altri media
- Senza il coinvolgimento dell'operatore di rete nel controllo o distribuzione del contenuto (chat, chiamate in video o in audio, servizi di video streaming)
- I servizi sono forniti sotto forma di applicazioni che eseguono il servizio di accesso ad Internet
- Gli operatori privati, spesso localizzati fuori dall'UE, trattano un'enorme quantità di dati personali che possono riguardare il contenuto o i metadati delle comunicazioni elettroniche

OBIETTIVO

- Autonomia nel controllo delle infrastrutture digitali del cloud e dei dati
- «*Il cloud italiano dovrà essere la casa sicura per i dati degli italiani che si devono fidare della Pa e dall'altro lato tutte le amministrazioni devono poter dare rapidamente e a costi ragionevoli i servizi per i cittadini*» (cit. Min. V. Colao, 7/9/21)

Per maggiori informazioni: c.luciani@gpdp.it