Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

Dati non personali, libera circolazione per rilanciare il cloud d'Europa

LINK: https://www.agendadigitale.eu/sicurezza/privacy/dati-non-personali-libera-circolazione-per-rilanciare-il-cloud-deuropa/

Dati non personali, libera circolazione per rilanciare il cloud d'Europa Home Sicurezza digitale Privacy Condividi questo articolo C'è un "gemello" meno conosciuto del Gdpr, ma altrettanto fondamentale per il Digital Single Market: il regolamento che punta a uno Schengen dei dati anonimi (ex ante o ex post), strategico per favorire il business transfrontaliero delle imprese. Ma serve che l'Italia si affretti a elaborare un framework normativo 1 minuto fa Giuseppe Vaciago Partner R&P Legal e fondatore di Tech&Law Center L'entrata in vigore del Regolamento europeo (1807/2018 del 14 novembre 2018) e la pubblicazione recente delle linee guida sui dati non personali sono in grado di aprire la strada a un vero e proprio mercato unico dell'UE dell'archiviazione e dell'elaborazione dei dati. E così creare un settore europeo di servizi di cloud competitivo, sicuro e affidabile e riducendo per gli utenti i prezzi dei servizi di archiviazione ed elaborazione dei dati. Norme importanti, quindi,anche se hanno avuto un clamore ben diverso dalla sorte spettata al 'gemello eterozigote' GDPR. L'auspicio di Andrus Ansip, Vicepresidente responsabile per il Mercato unico digitale, e di Mariya Gabriel, Commissaria responsabile per l'Economia e la società digitali, è quello di una crescita aggiuntiva del PIL dell'UE pari a 8 miliardi di euro l'anno. L'incipit del primo considerando del Regolamento è altrettanto di impatto quando afferma che: 'l'economia si sta velocemente digitalizzando. Le tecnologie dell'informazione e della comunicazione non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovativi e moderni. I dati elettronici sono al centro di tali sistemi e, quando sono analizzati o utilizzati in associazione a servizi e prodotti, possono generare un ingente valore. Allo stesso tempo, il rapido sviluppo dell'economia dei dati e di tecnologie emergenti come l'intelligenza artificiale, i prodotti e i servizirelativi all'Internet degli oggetti, i sistemi autonomi e la tecnologia 5G sollevano nuove questioni giuridiche relative all'accesso ai dati e al loro riutilizzo, alla responsabilità, all'etica e alla solidarietà'. Indice degli argomenti I tre capisaldi del regolamento Ue su dati non personali I limiti alla libera circolazione dati Circolazione dati non personali, l'ambito di applicazione La definizione di dato non personale Dati non personali, il divieto di localizzazione Portabilità dei dati: ultima data maggio 2020 I tre capisaldi del regolamento Ue su dati non personali 1. Il principio del libero flusso transfrontaliero di dati non personali. Gli Stati membri non possono più imporre alle organizzazioni di localizzare l'archiviazione o l'elaborazione dei dati all'interno dei propri confini. Le restrizioni saranno giustificate soltanto per motivi di pubblica sicurezza. Gli Stati Membri saranno tenuti a comunicare alla Commissione i requisiti già in vigore o nuovi in materia dilocalizzazione dei dati. Il libero flusso dei dati non personali renderà più facile e meno costoso per le imprese operare a livello transfrontaliero senza dover duplicare i sistemi informatici o salvare gli stessi dati in luoghi diversi.

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

Dal 30 maggio 2021 sarà sostanzialmente vietato imporre qualsiasi obbligo di localizzazione di dati. 2. Il principio della disponibilità dei dati per i controlli previsti dalla legge. Le autorità competenti potranno esercitare i diritti di accesso ai dati indipendentemente dal luogo di archiviazione o elaborazione nell'UE. Il libero flusso dei dati non personali non pregiudicherà gli obblighi delle imprese e delle altre organizzazioni di fornire determinati dati per i controlli previsti dalla legge. 3. Codici di condotta. Esattamente come è accaduto con il GDPR viene favorita l'elaborazione di codici di condotta a livello dell'UE per abolire gli ostacoli che impediscono di cambiare fornitore di servizi di archiviazione sul cloud o di ritrasferire idati nei sistemi informatici degli utenti. La soluzione di creare uno 'Schengen' dei dati non personali è sicuramente affascinante esattamente come è corretto promuovere un cloud più sicuro e affidabile, soprattutto ora che con l'avvento del GDPR vengono imposti degli standard di sicurezza più elevati e dei requisiti normativi non sempre di non facile applicazione per cloud provider extra UE. I limiti alla libera circolazione dati Pubblica Sicurezza. Il Regolamento all'articolo 5 prevede che la libera circolazione possa essere limitata per motivi di pubblica sicurezza. Il considerando 19 definisce 'pubblica sicurezza' ai sensi dell'articolo 52 TFUE, la sicurezza sia interna che esterna di uno Stato membro, come pure le questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati. In sostanza il concetto di 'pubblica sicurezza' presuppone l'esistenza di una minaccia reale e sufficientemente grave a uno degli interessifondamentali della società, quale il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari. Questa definizione seppur ampia può far nascere qualche dubbio sulla sua concreta applicazione. Basti pensare all'annosa questione della direttiva sulla 'Data Retention' e alle difformi interpretazioni che si sono susseguite. Attualmente tale normativa, che obbliga i fornitori di servizi di comunicazione elettronica (sostanzialmente gli Internet Service Provider) a conservare i file di log o gli indirizzi IP in caso di accertamento dei reati, vede la sua applicazione solo in alcuni Stati Membri, in quanto altri (Germania, Irlanda, Slovacchia, Bulgaria, Germania, Romania, Repubblica Ceca e Cipro) hanno dichiarato la legge di recepimento di tale Direttiva incostituzionale onon l'hanno mai applicata. In questo caso, il rischio potrebbe essere la difforme interpretazione tra uno Stato Membro e l'altro del concetto di pubblica sicurezza. Va detto che, ai sensi dell'articolo 7 dello stesso Regolamento, qualora, dopo avere richiesto l'accesso ai dati di un utente, un'Autorità competente non ottenga tale accesso, può chiedere l'assistenza di un'Autorità competente in un altro Stato membro secondo la procedura di cui all'articolo 7 del regolamento. Circolazione dati non personali, l'ambito di applicazione Il regolamento si applica alle attività di trattamento di dati elettronici diversi dai dati personali nell'Unione che (i) sono fornite come servizio ad utenti residenti o stabiliti nell'Unione, indipendentemente dal fatto che il fornitore di servizi sia o non sia stabilito

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

nell'Unione; (ii) sono effettuate da una persona fisica o giuridica residente o stabilito nell'Unione per le proprie esigenze. Da notare che a differenza del GDPR la persona fisica non èesclusa nel caso di esercizio di attività a carattere esclusivamente personale o domestico. Le linee guida fanno un esempio molto chiaro che merita di essere riportato: 'una piccola start-up europea dello Stato membro A decide di aumentare l'attività aprendo uno stabilimento nello Stato membro B. Per minimizzare i costi, la startup sceglie di centralizzare l'archiviazione e il trattamento dei dati del nuovo stabilimento nel suo server situato nello Stato membro A. Gli Stati membri non possono vietare questa iniziativa di centralizzazione IT, tranne se giustificata da motivi di pubblica sicurezza nel rispetto del principio di proporzionalità'. La definizione di dato non personale I dati vengono pragmaticamente definiti all'articolo 3 del testo, come tutti quei dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679. Il rimando fa intendere quanto le due normative sono inscindibilmente legate l'una con l'altra. I dati non personali possono essereclassificati in base alla loro origine come: Dati anonimi ex-ante: dati che in origine non si riferivano a una persona fisica identificata o identificabile, come i dati sulle condizioni meteorologiche prodotti da sensori installati sulle turbine eoliche o i dati sulle esigenze di manutenzione delle macchine industriali. Dati anonimi ex-post: dati che inizialmente erano dati personali, ma che poi sono stati resi anonimi. Le linee guida precisano che 'l'anonimizzazione dei dati personali è diversa dalla pseudonimizzazione, in quanto i dati che sono stati resi anonimi in modo adeguato non possono essere attribuiti a una persona specifica, neppure ricorrendo a informazioni aggiuntive e sono pertanto dati non personali. Questo aspetto è delicato perché garantire un corretto processo di anonimizzazione del dato non è semplice e non va sottovalutato da chi vuole percorrere questa strada per escludere l'applicazione dal GDPR'. È evidente che molto spesso ci si troverà di fronte ad un insiemedi dati misti, ossia contenenti sia dati personali che dati anonimi o non personali. In questo caso, il Regolamento non obbliga ad effettuare una segregazione del database 'misto' che sarà quindi soggetto agli obblighi dei due regolamenti per quanto di competenza. Un caso interessante di dati misti è fornito dai dati sanitari tra cui figurano le cartelle cliniche elettroniche, le sperimentazioni cliniche o gli insiemi di dati raccolti dalle varie applicazioni mobili per la salute e il benessere (come le applicazioni per misurare il proprio stato di salute, per ricordarci di prendere le medicine o per rilevare i progressi nella forma fisica). La divisione esatta tra dati personali e dati non personali in questi insiemi di dati sta diventando sempre più indistinta con gli sviluppi tecnologici. Pertanto, il loro trattamento deve essere conforme al regolamento generale sulla protezione dei dati, in particolare (dal momento che i dati sanitari rappresentano una categoria particolare didati secondo il regolamento) all'articolo 9 che stabilisce un divieto generale di trattamento di categorie particolari di dati e le eccezioni a questo divieto. I dati negli insiemi di dati misti contenenti dati sanitari possono essere una preziosa fonte d'informazione, ad es. per ulteriori ricerche mediche, per misurare gli effetti collaterali di un medicinale prescritto, per ottenere statistiche sulle malattie o

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

per sviluppare nuovi servizi o trattamenti sanitari. Tuttavia, occorre ottemperare al regolamento generale sulla protezione dei dati quando si effettua il trattamento iniziale nonché ulteriori trattamenti dei dati. Pertanto, un qualsiasi trattamento simile di dati sanitari deve avere una base giuridica valida e una motivazione adeguata ed essere sicuro di fornire garanzie di protezione sufficienti. Dati non personali, il divieto di localizzazione Per quanto attiene il punto più importante del Regolamento, l'articolo 4 del testo chiarisce che gli obblighi di localizzazione didati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità. Entro il 30 maggio 2021, gli Stati membri devono abrogare qualsiasi obbligo di localizzazione dei dati vigente stabilito da una legge, da un regolamento o da una disposizione amministrativa di carattere generale. Se invece tale Stato ritenesse che una vigente misura contenente un obbligo di localizzazione dei dati possa pertanto rimanere in vigore, comunicherà tale misura alla Commissione, giustificandone il mantenimento in vigore. La Commissione, entro un termine di sei mesi dalla data di ricevimento della comunicazione, esamina la conformità di tale atto con il Regolamento e, se del caso, presenta osservazioni allo Stato membro interessato con la raccomandazione di modificare o abrogare la misura. Un esempio fornito dalle linee guida è quello della contabilità del personale che per controllo regolamentare deve essere situata in uno specifico Stato membro perragioni riguardanti il controllo regolamentare, ad es. da parte dell'amministrazione fiscale nazionale. Tale normativa nazionale potrebbe essere in contrasto con il principio della libera circolazione. Tuttavia, sarà interessante vedere la capacità degli Stati Membri di collaborare in caso di accertamenti di natura giudiziaria. Portabilità dei dati: ultima data maggio 2020 Da ultimo, la Commissione incoraggia e facilita l'elaborazione di codici di condotta entro il 29 novembre 2019 e a dare loro effettiva attuazione entro il 29 maggio 2020 finalizzati a favorire: il cambio di fornitore di servizi e la portabilità dei dati in un formato strutturato, di uso comune e leggibile elettronicamente, anche in formati standard aperti ove necessario o richiesto dal fornitore di servizi che riceve i dati; gli obblighi d'informazione minimi per garantire che gli utenti professionali ricevano informazioni sufficientemente dettagliate, chiare e trasparenti prima della conclusione di un contratto ditrattamento di dati gli approcci in materia di sistemi di certificazione in materia di gestione della qualità, della sicurezza delle informazioni, della continuità operativa che agevolano il confronto di prodotti e servizi di trattamento dei dati per gli utenti professionali. Sotto questo profilo, un sottogruppo sta elaborando codici di autoregolamentazione sulla portabilità dei dati e sul cambio di fornitore di servizi cloud (gruppo di lavoro SWIPO), mentre un altro sottogruppo sta lavorando allo sviluppo della certificazione di sicurezza dei servizi cloud (gruppo di lavoro CSPCERT). In conclusione, l'applicazione pratica di questa normativa giocherà un ruolo davvero rilevante nella strategia di rilancio Europeo sul cloud fondato su concetti fondamentali: certezza giuridica e fiducia nel trattamento dei dati. Sarà interessante vedere se, nel lungo periodo, tale approccio risulterà vincente rispetto a chi non ha ancora

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

messo in piedi un framework normativo di tale portata. L'Italia èavvisata: potrebbe essere l'ultimo appello per un serio rilancio nel settore che può avvenire solo attraverso investimenti oculati e grande attenzione alla compliance normativa.