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

OVH, attenzione ai contratti cloud: la lezione per il titolare trattamento dati

LINK: https://www.agendadigitale.eu/sicurezza/privacy/ovh-attenzione-ai-contratti-cloud-la-lezione-per-il-titolare-trattamento-dati/

OVH, attenzione ai contratti cloud: la lezione per il titolare trattamento dati Home Sicurezza digitale Privacy L'incendio del datacenter OVH e i relativi problemi sui siti e servizi ospitati in cloud è lezione utile per ricordare le cautele che occorre seguire nella fase di stipula del contratto col fornitore del servizio. E le possibili conseguenze, anche sanzionatorie, di violazione del Regolamento UE 2016/679 (GDPR) 6 secondi fa Laura Mantelli & Lee de Bedin & Lee studio legale associato Il rogo divampato nella notte tra il 9 e 10 marzo nel sito del data center di OVH a Strasburgo ha avuto conseguenze dirette ed importanti per molte aziende e pubbliche amministrazioni, anche italiane, con siti web off line ed impossibilità di utilizzo dei servizi ed accesso ai dati contenuti nel cloud. Solo per citare alcuni esempi, in Italia hanno registrato disservizi il Comune di Pavia, la Città di Trapani, il Comune di Cattolica; in Francia, il centro nazionale d'arte Pompidou, ma anche, nel resto d'Europa, la piattaforma di blogging e di scambio di criptovalute Deribit e l'agenzia stampa eeNews Europe, e molti molti altri. Indice degli argomenti L'importanza del contratto cloud Privacy e cloud Che deve fare il titolare del trattamento Il back up Il luogo del server del fornitore cloud Clausole contrattuali su risarcimento dnno In conclusione L'importanza del contratto cloud L'accaduto, al momento non ancora chiaro nelle sue conseguenze e nella durata dei disservizi (OVH ha promesso il restart dei data center tra il 15 ed il 19 marzo, con un pieno recupero nell'arco delle prossime due settimane), ha riacceso i riflettori sul cloud computing, molto comodo e utile per le aziende, pubbliche e private, ma con profili di criticità e rischi nell'ambito della data protection, a causa del pericolo di perdita di controllo dei propri dati; è, dunque, utile ricordare le cautele che occorre porre in essere nella fase di stipula del contratto col fornitore del servizio e le possibili conseguenze, anche sanzionatorie, di violazione del Regolamento UE 2016/679 (GDPR). Privacy e cloud Dal punto di vista privacy, l'ente pubblico o l'azienda privata che si rivolgono ad un fornitore esterno di servizi cloud e trattano dati di persone fisiche (loro clienti o utenti) sono qualificati come "titolari del trattamento" e devono procedere a designare il fornitore di tali servizi quale "responsabile esterno del trattamento" ex art. 28 GDPR; il Titolate del Trattamento deve porre particolare attenzione a questa fase contrattuale, non solo inserendo tutte le clausole previste come obbligatorie dal citato art. 28, ma altresì avendo cura di verificare che le garanzie e le misure di sicurezza offerte dal fornitore siano

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

idonee alla protezione dei dati. E ciò, nell'ottica sia di salvaguardare i propri dati aziendali (di natura personale o anche non personale), che rappresentano in molti casi l'asset più importante per una società, sia di evitare possibili sanzioni: va infatti rammentato che, in caso di violazioni commesse del fornitore del sistema cloud, anche il titolare del trattamento sarà chiamato a rispondere dell'eventuale illecito. E' pur vero che spesso i titolari del trattamento, ed in special modo se di piccole dimensioni, non hanno potere contrattuale tale da consentire loro di pretendere che il fornitore del cloud inserisca nel contratto standard dallo stesso (di norma unilateralmente predisposto) clausole e garanzie particolari così come sistemi e misure aggiuntive di sicurezza. Va però evidenziato che questa pur oggettiva circostanza non costituisce un'esimente da una possibile responsabilità nel caso di violazione della normativa privacy: il titolare del trattamento ha sempre la possibilità, ed anzi deve, rivolgersi al fornitore che offre maggiori garanzie. Che deve fare il titolare del trattamento In fase contrattuale e di redazione della nomina di un fornitore quale responsabile esterno del trattamento, il titolare del trattamento deve, dunque, verificare attentamente quali sono le misure di sicurezza adottate dal fornitore (in questo caso, cloud provider) per proteggere i dati: al riguardo, il fornitore dispone generalmente di sistemi di protezione contro virus, attacchi hacker o altri pericoli informatici. Il caso OVH ha, però, insegnato che non ci si deve mai dimenticare della sicurezza fisica dei luoghi ove si trovano i server informatici; probabilmente, negli ultimi anni si è posta maggiore attenzione alla sicurezza informatica, pensando meno alla circostanza che è altrettanto (se non di più) importante la sicurezza fisica dei luoghi. WHITEPAPER Come è cambiato in Italia il quadro normativo dei pagamenti digitali verso la PA? Scarica il Whitepaper Inoltre, occorre verificare che il fornitore abbia adottato un idoneo recovery plan, per il caso di attacchi informatici o calamità naturali che comportino problemi di connessione, perdita di dati eccetera. Per tali evenienze, il titolare del trattamento deve anche effettuare una valutazione dell'impatto che perdite di dati o impossibilità temporanea di accedere agli stessi hanno sulla propria attività e sui tempi di recupero del sistema. In particolare, devono porre attenzione a questo aspetto le realtà che offrono servizi continuativi essenziali, che non possono permettersi un'inattività prolungata. E', dunque, necessario che il titolare del trattamento valuti con attenzione le conseguenze sulla propria organizzazione dell'eventuale interruzione, di durata più o meno lunga, del servizio offerto, calcolando i costi diretti ed indiretti dell'inaccessibilità ai dati e definire in anticipo il piano di emergenza e recupero. Il back up Essenziale è adottare è un idoneo sistema di backup che consenta sempre di accedere e recuperare i dati, anche nel caso di inaccessibilità al sistema cloud; è, dunque, molto importante che il sistema di backup sia separato, fisicamente e informaticamente, rispetto al sistema "principale", in modo che non possa anch'esso risentire di eventuali problemi subiti dal cloud. Ad esempio, nel caso dell'incendio OVH pare che molti clienti facessero affidamento sul servizio di backup fornito dallo stesso OVH al momento, per molti, anch'esso inutilizzabile, con conseguente inutilità di avere un sistema di backup siffatto e perduranti problemi di inaccessibilità ai dati. Il luogo del server del

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

fornitore cloud Molta attenzione devono poi porre i titolari del trattamento sul luogo di ubicazione dei server del fornitore di cloud, in particolare sul fatto se i server siano allocati in Unione Europea oppure in Paesi Extra UE (problema, questo, che non si pone per il caso di OVH, i cui server sono appunto situati a Strasburgo, in Francia). Infatti, il GDPR (articoli 44 e seguenti) consente il trasferimento dei dati nei Paesi Extra UE solo a condizione che l'adeguatezza del Paese Extra UE o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 del GDPR), oppure in assenza di tale decisione, ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 GDPR). E ciò va preso particolarmente in considerazione soprattutto dopo che la Corte di Giustizia Europea il 16 luglio 2020 con la sentenza Schrems II (C-311/18) ha annullato la decisione 2016/1250 della Commissione Europea che aveva affermato l'adeguatezza del Privacy Shield (il regime dello scudo UE-USA). Clausole contrattuali su risarcimento dnno Infine, molto utili a tutela del titolare del trattamento (anche se ovviamente difficilmente ottenibili in un normale rapporto contrattuale tra la piccola impresa ed il fornitore di cloud) sono le clausole contrattuali che prevedono un diritto di risarcimento del danno o di manleva da parte del fornitore del cloud o ancora clausole penali per il caso di incidenti e malfunzionamenti che rechino perdita dei dati e possano comportare sanzioni e richieste risarcitorie da parte degli interessati. Assai utile, e da valutare positivamente nell'ambito della scelta del fornitore cloud, è la presenza di un'idonea polizza assicurativa che possa coprire gli eventuali danni per il caso di incidente. Da ultimo, occorre non dimenticare che il titolare del trattamento ha, ai sensi dell'art. 28, lett. h) del GDPR, il diritto (che, però, si trasforma anche in un dovere) di effettuare ispezioni presso il nominato responsabile esterno del trattamento, al fine di verificare il rispetto degli obblighi di cui al GDPR ed al contratto sottoscritto. In conclusione Le brevi osservazioni che precedono evidenziano comunque l'assoluta centralità dei temi relativi alla sicurezza del cloud, alla perdita dei dati ed all'impossibilità di loro recupero in quanto potenzialmente implicanti una violazione del GDPR, con ogni conseguenza sanzionatoria. Va infatti ricordato in particolare che l'art. 32 del GDPR prevede che tanto il titolare del trattamento quanto il Responsabile esterno del Trattamento sono tenuti a mettere in atto misure "tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" sempre "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità di trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche". Più in dettaglio, l'art. 32, alle lettere b) e c), prevede espressamente che ciascuno di essi debba garantire la capacità di assicurare in via permanente l'integrità e la disponibilità dei sistemi e dei servizi di trattamento dei dati, nonché quella di ripristinare "tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico". WHITEPAPER Gestione dei contratti e GDPR: guida all'esternalizzazione di attività dei dati personali

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

Legal Scarica il Whitepaper In conclusione per tornare, esemplificativamente, all'evento che ha dato occasione a queste brevi riflessioni, il rogo nel data center OVH potrebbe comportare l'applicazione di sanzioni sia nei confronti di OVH sia nei confronti di tutte le aziende, pubbliche e private, clienti della stessa OVH, qualora emergesse, all'esito delle verifiche che verranno condotte, una violazione delle misure di sicurezza oppure un'incapacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali. @RIPRODUZIONE RISERVATA