Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

AL24

PROCEDURA INTERNA VOLTA ALLA VALUTAZIONE PRELIMINARE DI QUALSIASI SERVIZIO ICT

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE, (P. IVA: 09323530965) (infra "ASST RHODENSE"), in persona del suo legale rappresentante pro tempore, con sede legale in Garbagnate Milanese (MI), viale Forlanini, 95, intende illustrare – in ossequio al combinato disposto tra gli artt. 5 paragrafo 2), 24 paragrafi 1) e 2) e 25 del Regolamento UE n. 2016/679 (GDPR) – gli elementi rilevanti della normativa comunitaria (e nazionale) sulla protezione dei dati personali (data protection/privacy) che, in qualità Titolare del trattamento ex artt. 4 n. 7) e 24 del GDPR, debbono essere presi in considerazione laddove si decide di usufruire di **QUALSIASI SERVIZIO ICT**, ivi incluso il servizio di cloud computing (CSP).

Premessa.
Quanto verrà, di seguito, illustrato è il risultato dell'analisi della "Guida all'uso del cloud" pubblicata, a Marzo 2022, dal Garante per la protezione dei dati personali danese (Datatilsynet), da leggersi, (sempre) in combinato disposto, con il Parere n. 17/2021, il Parere n. 16/2021, le Linee Guida n. 4/2021, le Linee Guida n. 5/2021, la Raccomandazione n. 1/2020, la Raccomandazione n. 2/2020, le Linee Guida n. 2/2020, le Linee Guida n. 2/2018, il Parere n. 254/2018, il Documento di Lavoro n. 1/2016 e il Parere n. 4/2014, tutti a firma dell'EDPB (già WP Art. 29).

Ancor prima di descrivere, nel dettaglio, le peculiari criticità che un Titolare del trattamento deve tenere in considerazione laddove decide di impiegare un servizio ICT/CSP (poi da regolamentare mediante il consueto atto di nomina a Responsabile del trattamento ex art. 28 del Regolamento UE n. 2016/679[1]), occorre ricordare, in via preliminare, che un CSP si compone di una serie di tratti distintivi, sia di carattere oggettivo/funzionale (IaaS[2]; PaaS[3]; SaaS[4]) sia di carattere soggettivo (privato[5]; condiviso[6]; pubblico[7]; ibrido[8]).

Passaggio n. 1): stabilire un livello adeguato di sicurezza dell'operazione di trattamento in esame.
Tanto premesso, il Datatilsynet evidenzia, in primo luogo, la necessità di stabilire un livello (adeguato) di sicurezza nel trattamento valutato sulla base dei rischi per i diritti e le libertà del soggetto interessato coinvolto nell'operazione di trattamento da prendere in considerazione, onde così identificare, anche grazie all'eventuale assistenza del relativo fornitore ICT/CSP, quale livello di sicurezza del trattamento ha stabilito il fornitore ICT/CSP (se del caso, anche grazie al dialogo o all'esame della documentazione rilasciata da quest'ultimo) e, di conseguenza, esaminare (e, poi,

[1] Per i requisiti minimi e gli ulteriori dettagli da inserire nell'accordo di trattamento, si consiglia di far riferimento, oltre ovviamente al dettato normativo applicabile, anche ai modelli contrattuali predisposti, sul punto, sia dal Garante privacy danese medesimo sia dalla Commissione UE in data 7.6.2021, ai sensi dell'art. 28, paragrafo 7), del GDPR.
[2] Infrastructure-as-a-Service (IaaS) offre un primo livello di delega della gestione dell'infrastruttura on-premise. Si tratta di un servizio con modello di consumo pay-as-you go, in cui una terza parte fornisce i servizi di infrastruttura come lo storage e la virtualizzazione quando sono necessari, tramite cloud e Internet.
[3] Platform-as-a-Service (PaaS) offre un ulteriore livello di astrazione rispetto alla gestione completa e on premise dell'infrastruttura; prevede che hardware e software siano ospitati nell'infrastruttura del provider, che distribuisce la piattaforma all'utente come soluzione integrata, stack di soluzioni o servizio erogato tramite una connessione internet.
[4] Software-as-a-Service (SaaS), anche noto come servizi applicativi cloud, è la forma più completa di servizi di cloud computing, e consiste nella fornitura di un'intera applicazione gestita da un provider tramite un browser web; il provider si occupa degli aggiornamenti software, della correzione dei bug e di altre attività generiche di manutenzione del software, mentre l'utente si connette all'app tramite un'API o dashboard.
[5] CSP ad uso esclusivo di una singola e specifica organizzazione.
[6] CSP ad uso esclusivo di un gruppo imprenditoriale definito.
[7] CSP tipicamente offerto, ad una generalità di destinatari, a condizioni commerciali predefinite.
[8] CSP è il risultato di una combinazione di due o più servizi cloud differenti (privato; pubblico; condiviso).

documentare) se il livello di sicurezza rilevato corrisponde a quello che, in qualità di Titolare del trattamento, viene considerato appropriato ed accettabile.

Passaggio n. 2): effettuare uno screening del potenziale fornitore ICT/CSP.
Il secondo passaggio consiste, invece, nell'effettuare, in anticipo, un accurato screening del potenziale fornitore ICT/CSP, al fine così di valutare se questi è in grado, o meno, di soddisfare i requisiti di protezione dei dati personali considerati appropriati per l'operazione di trattamento di specie, anche grazie alla sottoposizione, nei suoi

confronti, di un apposito questionario, vertente, inter alia, sulle seguenti tematiche individuate dal Garante privacy danese:

i. Il fornitore ICT/CSP ha l'obbligo di elaborare i dati personali solo in base alle istruzioni documentate del relativo Titolare del trattamento oppure si riserva il diritto di elaborare i dati personali anche per propri scopi?
ii. Il fornitore ICT/CSP assicura, tramite apposite politiche e procedure, che il proprio personale dipendente o similare si è impegnato alla confidenzialità e alla riservatezza dei dati personali oggetto di trattamento?
iii. Il fornitore ICT/CSP ha stabilito un appropriato livello di sicurezza del trattamento rispetto all'attività di trattamento che si intende affidare?
iv. Il fornitore ICT/CSP dispone di una procedura per esaminare i propri (sub) Responsabili del trattamento ex art. 28, paragrafo 4), del GDPR? L'accordo con il relativo (sub) Responsabile del trattamento, laddove esistente, riflette i medesimi requisiti imposti al fornitore ICT/CSP dal Titolare del trattamento?
v. Il fornitore ICT/CSP dispone di un quadro completo dei (sub) Responsabili del trattamento utilizzati per la fornitura dei propri servizi (cd. catena/gerarchia di approvvigionamento), ivi inclusi i paesi (anche extra SEE) in cui si trovano ovvero da cui possono accedere ai dati personali? In caso di risposta affermativa, il fornitore ICT/CSP ha stabilito uno strumento di trasferimento efficace?
vi. In relazione all'attività di trattamento da affidare, il fornitore ICT/CSP dispone di procedure per assistere il Titolare del trattamento nella gestione delle richieste dei soggetti interessati ai sensi del Capo III) del GDPR?
vii. Il fornitore ICT/CSP possiede delle procedure volte alla gestione di una violazione di dati personali, ivi inclusa l'assistenza, in merito, in favore del relativo Titolare del trattamento?
viii. Il fornitore ICT/CSP può, tenuto anche conto delle disposizioni normative applicabili, cancellare ovvero restituire al Titolare del trattamento i dati personali al termine delle operazioni di trattamento demandate?
ix. Il fornitore ICT/CSP possiede una procedura mirata ad assistere il Titolare del trattamento nello svolgimento di un eventuale audit ovvero volta ad effettuare un audit da parte di terzi soggetti indipendenti?

Passaggio n. 3): determinare la frequenza e la tipologia dell'audit, ove necessario.
Il terzo aspetto da tenere in considerazione consiste nel valutare la frequenza (e la modalità) dell'audit da svolgere nei confronti del relativo fornitore ICT/CSP, aspetti da calibrare sulla base della valutazione circa i rischi (per i diritti e le libertà) dei soggetti interessati coinvolti nella specifica operazione di trattamento.

In proposito, il Datatilsynet ha individuato una serie di fattori che indicano la necessità di svolgere, nei confronti del fornitore ICT/CSP, un audit con una frequenza maggiore (es. difficoltà, in passato, di rispettare determinati accordi contrattuali; sostituzione frequente dei propri (sub) Responsabili del trattamento; frequenti acquisizioni, cambi di proprietà, fusioni ovvero cambiamenti significativi nella strategia aziendale del fornitore ICT/CSP; registrazione di diverse violazioni di dati personali) ovvero minore (es. lunga esperienza sintomatica di un servizio stabile, caratterizzata dall'assenza (o comunque da un numero esiguo) di violazioni di dati personali).

A tal riguardo, il Garante privacy danese ha, ulteriormente, precisato che, laddove l'audit, nei confronti del relativo fornitore ICT/CSP, venga svolto da un soggetto terzo indipendente, può risultare sufficiente, per il Titolare del trattamento, l'analisi del relativo rapporto, a condizione che esso riguardi, invero, anche le attività di trattamento materialmente affidate al fornitore ICT/CSP, consigliando, così, in caso contrario, di ottenere contrattualmente la facoltà di svolgere un audit avente un differente ambito applicativo.

Passaggio n. 4): analisi degli eventuali trasferimenti di dati personali verso paesi extra SEE.

Infine, l'ultimo elemento da valutare sussiste laddove il Titolare del trattamento decide di utilizzare un fornitore ICT/CSP che si trova in un paese extra SEE (cd. paese terzo) ovvero che impiega uno o più (sub) Responsabili del trattamento situati al di fuori del SEE (anche solo per l'esecuzione di funzioni di servizio o supporto, ovvero per la risoluzione di problemi all'infrastruttura del fornitore ICT/CSP) ovvero stabilito nell'UE ma che, in ragione della propria struttura societaria, è soggetto al "Clarifying Lawful Overseas Use of Data Act" americano (Cloud Act).

In tal caso, il Titolare del trattamento deve fare affidamento sulle prescrizioni espresse, sul punto, dall'EDPB (a partire, dalle più recenti Raccomandazioni n. 1 e 2 del 2020)[9], e, in particolare, deve effettuare, senz'altro, i seguenti adempimenti: (i) identificare i trasferimenti di dati personali verso un paese terzo; (ii) identificare o stabilire lo strumento di trasferimento pertinente su cui fare affidamento; (iii) valutare se lo strumento di trasferimento ex art. 46 del GDPR su cui fare affidamento è, o meno, efficace alla luce di tutte le specifiche caratteristiche del trasferimento e, in caso contrario, adottare misure supplementari (tecniche; organizzative; contrattuali); (iv) rivalutare, ad intervalli appropriati, i trasferimenti effettuati.

Al tal proposito, il Datatilsynet ha, da ultimo, provveduto ad illustrare una serie di utili (e pratici) suggerimenti, quali:

- ✓ Se il Titolare del trattamento non è in grado di dialogare con il fornitore ICT/CSP ovvero se il dialogo con quest'ultimo non consente la raccolta di informazioni sufficienti per poter documentare quali specifici (sub) Responsabili del trattamento (e in quali luoghi essi sono stabiliti) sono rilevanti per i servizi utilizzati, il primo è tenuto a presumere che tutti i (sub) Responsabili del trattamento, indicati nell'elenco del fornitore ICT/CSP, vengono impiegati per la fornitura del servizio di cloud computing di specie.
- ✓ Nel caso in cui vi sono leggi e/o prassi del paese terzo idonee a permettere la raccolta o l'accesso ai dati personali oggetto di trasferimento da parte dell'autorità di polizia in una modalità tale da non soddisfare i criteri già espressi nella recente (e famosa) sentenza C-311/2018 (cd. Schrems II) della Corte di Giustizia dell'Unione Europea (CGUE), il Titolare del trattamento possiede tre opzioni, così come già illustrate dall'EDPB: (i) astenersi dall'iniziare il trasferimento ovvero sospendere il trasferimento; (ii) adottare misure supplementari efficaci (perlopiù, tecniche: es. crittografia; pseudonimizzazione; split processing), al fine di assicurare un livello di protezione sostanzialmente equivalente a quello garantito dalla Carta dei diritti fondamentali dell'UE (Carta): a tal riguardo, il Garante privacy danese ha precisato che, dinnanzi al teorico obbligo di valutare la legislazione e la prassi di un'ampia gamma di paesi terzi ove sono stabiliti i (sub) Responsabili del trattamento utilizzati dal fornitore ICT/CSP, il Titolare del trattamento può adottare il criterio del "worst case" (ossia che tutti i paesi terzi, oggetto di valutazione, possiedono una legislazione/prassi problematica rispetto alle tutele previste dalla Carta) e, dunque, valutare e, poi, individuare quali misure tecniche supplementari possono essere efficacemente attuate al fine di garantire un livello di protezione essenzialmente equivalente a quello prescritto dalla Carta; (iii) continuare il trasferimento senza la preventiva adozione di misure supplementari, se si ritiene che, in base ad un analisi obiettiva ed affidabile, i dati personali, oggetto di trattamento, non sono interessati dalla legislazione/prassi del paese terzo.

Garbagnate Milanese, lì 9.11.2022 (data di ultimo aggiornamento).

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE
(in persona del suo legale rappresentante pro tempore)

[9] Per maggiori approfondimenti, si rimanda all'apposita policy vertente sul trasferimento di dati extra SEE.