UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Transfert impact assessment

Gaspare Staniscia
staniscia64@gmail.com

Martedì 19 settembre 2023

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Case of study

La ditta Alfa, società multinazionale operante nel campo dei dispositivi medici e con sede negli Usa, si aggiudica, per il tramite della sua filiale italiana, la fornitura in service di strumentazioni varie per le analisi di laboratorio da installare presso l'Azienda Ospedaliera di Valle Grande.
L'apparecchiatura, tra l'altro, dispone di un sistema di connessione remota (per malfunzionamenti particolarmente critici) con i tecnici di casa madre (in USA) che comunque si appoggiano all'occorrenza su server allocati in UE. Ad oggi Alfa non aderisce alla recente Decisione di Adeguatezza del 10 luglio '23.

argomenti

- organigramma privacy, gli adempimenti:

a) DPIA ex art. 35 GDPR;

b) DPA + SCC con validità di un anno e con riserva, per il Responsabile del trattamento, di aderire *medio tempore* alla Decisione di Adeguatezza del 10 luglio 2023;

- sentenza CGUE del 16/07/2020 c.d. Schrems II;
- recente evoluzione dello scenario internazionale (E.O. n. 14086/Trans Atlantic Privacy Framework);
- perplessità manifestate dall'EPBD parere del 28 febbraio 2023;
- perplessità manifestate del Parlamento Europeo risoluzione del 11 maggio 2023;
- la Decisione di Adeguatezza del 10 luglio 2023.

argomenti

- accountability del Titolare/Valutazione d'impatto del trasferimento (TIA):

1. analisi del trattamento (estratto doc artt.28, 30,35 GDPR);
2. identificare lo strumento di trasferimento su cui si fa affidamento (estratto SCC All. IA, All. IB, All. IC; All. II; All. III);
3. valutare se lo strumento di trasferimento invocato è efficace alla luce delle circostanze di trasferimento (FISA Section 702, EO 1233 e Cloud Act/trasparency report negativo);
4. identificare le misure tecniche, contrattuali e organizzative applicate per proteggere i dati (data center in UE, misure di cui al DPA ed SCC);
5. valutazione finale;
6. rivalutare a intervalli appropriati.

organigramma privacy
gli adempimenti

Tra l'A.O. di Valle Grande e la Ditta Alfa si instaura il rapporto Titolare/Responsabile del Trattamento dati che sarà regolato dalla stipula di un accordo ex art 28 GDPR.

Stante la sussistenza delle seguenti fattispecie, si ritiene di procedere alla redazione di una DPIA ex art. 35 GDPR:

- Art. 35 par 3 lett. b) trattamento su larga scala di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 idonei a rivelare lo stato di salute degli interessati;

organigramma privacy
gli adempimenti

- Wp 248 (linee guida Gruppo Art. 29) valutazioni ex n.5 circa:
- numero di soggetti interessati (espressi in percentuale rispetto alla popolazione di riferimento: AO di Valle Grande è Centro Nazionale di Eccellenza per le patologie rare ematologiche);
- volume dei dati: il Titolare esegue oltre 2.000.000 di prestazioni sanitarie di laboratorio analisi all'anno;
- durata dell'attività di trattamento: destinata a persistere per molti anni;
- estensione geografica dell'attività di trattamento che è nazionale.

- Wp 248 (linee guida Gruppo Art. 29) n. 7:
- valutazione circa lo status di vulnerabilità dell'interessato: i dati trattati riguardano soggetti vulnerabili (bambini, dipendenti, soggetti con patologie psichiatriche, richiedenti asilo, anziani e **pazienti**, etc);
- Valutazioni ex Provv. Garante n. 467 del 11/10/2018 n.6:
- trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, **pazienti**, richiedenti asilo);

organigramma privacy
gli adempimenti

- Il trattamento delineato implica, nell'ambito dell'attività di troubleshooting di secondo livello, il trasferimento transfrontaliero di dati (con destinazione USA) che possono contenere informazioni sanitarie dei pazienti pertanto si rendono necessarie le considerazioni in appresso effettuate.

sentenza CGUE del 16/07/2020 c.d. Schrems II

Elementi giuridici comunitari di riferimento:

- sentenza CGUE del 16/07/2020 (c.d Schrems II) che da un lato ha caducato la Decisione di adeguatezza adottata nel 2016 dalla Commissione Europea (c.d. Privacy Shield) in seguito alla decadenza del precedente accordo di Safe Harbor, ma dall'altro ha ritenuto ancora valida la decisione n. 2010/CGUE circa la utilizzabilità delle SCC.

Elementi giuridici afferenti la legislazione statunitense:

- Section 702 Foreign Intelligence Surveillance Act (FISA);
- Executive Order (EO) 12333;
- Cloud Act.

recente evoluzione dello scenario internazionale (E.O. n. 14086/Trans Atlantic Privacy Framework)

- Marzo 2022 annuncio Biden/Von Der Leyen;
- 7 ottobre 2022, l'Executive Order del Presidente USA Joe Biden n. 14086 rimette in moto il Dialogo USA-UE. L'ordine esecutivo, in particolare impone:
- la ridefinizione dei limiti di accesso da parte dell'intelligence statunitense ai dati, con limitazioni in termini di **necessità** e **proporzionalità;**
- l'istituzione di un nuovo meccanismo di ricorso indipendente e imparziale, accessibile anche ai cittadini non statunitensi, il **Data Protection Review Court** (DPRC).

recente evoluzione dello scenario internazionale (E.O. n. 14086/Trans Atlantic Privacy Framework)

- Il protocollo internazionale che nasce dal suddetto atto presidenziale, il «Trans-Atlantic Data Privacy Framework», contiene inoltre le seguenti garanzie:

a) le agenzie di intelligence USA dovranno adottare delle procedure per assicurare un'efficace supervisione dei nuovi standard privacy;

b) obblighi stringenti per le aziende (i c.d. importatori) che trattano i dati personali trasferiti dall'Unione Europea, con obbligo di autocertificare il rispetto dei nuovi principi attraverso il Dipartimento del Commercio degli Stati Uniti;

c) specifici meccanismi di monitoraggio e revisione.

perplessità manifestate dall'EPBD parere del 28 febbraio 2023

L'EDPB nel suo parere n.5 del 28 febbraio 2023, pur riconoscendo gli importanti miglioramenti nel quadro di riferimento, ha espresso perplessità in relazione:

- alla fonte normativa utilizzata (atto presidenziale non legge federale);
- alla non esatta determinazione degli strumenti di ricorso previsti in favore degli interessati UE;
- alla reale indipendenza della DPRC.

perplessità manifestate dal Parlamento Europeo risoluzione del 11 maggio 2023

- Con la risoluzione dell'11 maggio 2023, il Parlamento Europeo sulla questione ha affermato che il Data Privacy Framework costituisce un miglioramento rispetto al Privacy Shield, ma non sufficiente al fine di approvare una decisione di adeguatezza sul trasferimento di dati personali.

la Decisione di Adeguatezza del 10 luglio 2023

- la Commissione Europea giunge alla conclusione che gli Stati Uniti garantiscono un livello di protezione adeguato e comparabile a quello dell'Unione Europea;
- prossime tappe previste dallo strumento ex art. 45 GDPR: il funzionamento del quadro UE-USA per la protezione dei dati personali sarà oggetto di riesami periodici effettuati dalla Commissione Europea in collaborazione con i rappresentanti delle autorità europee di protezione dei dati e delle autorità statunitensi competenti. **Il primo riesame avrà luogo entro un anno dall'entrata in vigore della decisione di adeguatezza e verificherà che tutti gli elementi pertinenti siano stati pienamente attuati nel quadro giuridico statunitense e funzionino efficacemente nella pratica.**

accountability del titolare/ TIA

- PREMESSA: alla luce dei rilievi esposti fino ad ora, il Titolare, pur conoscendo la recente Decisione di Adeguatezza EU-USA, ai sensi degli artt. 5 e 24 GDPR, interloquisce con il proprio Responsabile/importatore che non risulta ancora iscritto nella Data Privacy Framework List e reputa necessario compiere una valutazione d'impatto del trasferimento dei dati.

1. Analisi del trattamento (ci si riporta in estratto alla documentazione ex artt.28/30/35 GDPR): Alfa rispetta gli obblighi assunti con la sottoscrizione del DPA ed offre la sua completa collaborazione alla redazione della prescritta Valutazione ex art 35 GDPR. La documentazione fornisce le seguenti informazioni:

accountability del titolare/TIA

all A DPA/ art 30 GDPR par 1

Nome e dati di contatto del Titolare e del suo RPD	**AO di Valle Grande corr. in XYZ, info@aovallegrande.it,** **DPO dott. Mario Rossi corr in XXX, dpo@aovallegande.it**
Nome e dati di contatto del Responsabile e del suo RPD	Alfa spa corr. In ZZZZ - USA DPO Richard Smith dpo@alfa.com
Natura e finalità del trattamento	fornitura in service di attrezzatture e sistemi analitici art 9 par 2 lett (h; GDPR art 6 par 1 lett (c GDPR
Categorie di soggetti interessati	pazienti della AO di Valle Grande
Tipologie di dati personali coinvolti	dati comuni e dati particolari circa lo stato di salute
Categorie di destinatari dei dati	soggetti autorizzati dal titolare e dal Responsabile,
Trasferimento dei dati extra-UE	USA/SCC
Durata del trattamento	durata contrattuale/cancellazione secondo massimario di scarto
Misure di sicurezza adottate	All. C
Valutazione dei rischi del trattamento	Si
Valutazione d'impatto sulla protezione dei dati	Si

accountability del titolare/ TIA

- All. B DPA

Indicazione dei sub responsabili ex art 28 par 2 RGDP

ID	Ragione sociale	Sede legale	E-mail/PEC	Recapito del DPO	Ambito di trattamento
1	server spa	Luxemburg	server@legalmail.com	xxxxxx	gestione server Z

ADDENDUM ALL'ACCORDO PER IL TRATTAMENTO (ex *art. 28 GDPR)*

incarico di amministratore di sistema con designazione ADS ex Provv. Gen. dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 recante *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* (G.U. n. 300 del 24 dicembre 2008) e successive specifiche integrazioni nei confronti dei seguenti soggetti:

ID	Nome e Cognome	Ragione Sociale	Recapito E-mail/Telefono	Sistemi Amministrati
1	Giuseppe Verdi	server spa	giuseppe.verdi@server.con	alfa lab
2	Paolo Bianchi	server spa	paolo.bianchi@server.com	alfa lab
3	Jhon Deer	server spa	jhon.deer@server.com	server Z
4	Will Smith	server spa	will.smith@server.com	server Z
5	Paul Walker	alfa spa	paul.walker@alfa.com	alfa lab
6	Joe Curuma	alfa spa	joe.curuma@alfa.com	alfa lab

accountability del titolare/ TIA

- All C DPA Tom's del Responsabile

Certificazione ISO 27001; Certificazione ISO 27701; Certificazione 27017; Nomina DPO; istruzioni art 29 GDPR/Formazione annuale privacy dei dipendenti;
Adozione policy ex artt. 12/22 GDPR per cancellazione, rettifica, aggiornamento, limitazione del trattamento e portabilità dei dati personali su richiesta del titolare; Adozione policy ex art 33 par 2 GDPR; Tenuta registro trattamenti del Responsabile;
Crittografia dei dati inattivi e in transito; Residenza dei dati su datacenter europei;
Riesame annuale dei profili di accesso; immediata cancellazione delle copie di back up dopo gli interventi;
Rispetto linee guida AGID per trattamento dei dati critici su cloud non certificati.

accountability del titolare/ TIA

- Estratto DPIA

Informazioni generali del trattamento	
Denominazione del trattamento	TR1
Descrizione del trattamento	diagnostica medica per il tramite di apparecchiature di laboratorio in service
Natura del trattamento	medico diagnostico
Ambito di applicazione	sanitario
Contesto	responsabilità medica/responsabilità appaltatore
Finalità	diagnosi e cura
Dati personali	particolari (stato di salute) comuni (identificativi)
Destinatari	soggetti autorizzati dal titolare/Soggetti autorizzati dal Responsabile del trattamento/interessati
Periodo di conservazione	nel rispetto del massimario di scarto adottato dal titolare, e nel rispetto dei termini contrattuali con l'appaltatore reperiti nel DPA
Autorizzati	nel rispetto della policy interna del titolare (xx) /nel rispetto degli obblighi assunti dal Responsabile nel DPA
Asset coinvolti	LIS/server esterni Z
Codici di condotta adottati (arti. 35, par. 8)	no

accountability del titolare/ TIA

Motivo della redazione DPIA	• **Art. 35 par 3 lett. b) trattamento su larga scala di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, idonei a rivelare lo stato di salute degli interessati;** • **Wp 248 (linee guida Gruppo Art. 29) valutazioni ex n.5 circa:** - **numero di soggetti interessati espressi in percentuale rispetto alla popolazione di riferimento: AO di Valle Grande è Centro Nazionale di Eccellenza per le patologie rare ematologiche;** - **volume dei dati oggetto di trattamento: il Titolare esegue oltre 2.000.000 di prestazioni sanitarie di laboratorio analisi all'anno;** - **durata dell'attività di trattamento;** - **estensione geografica dell'attività di trattamento che è nazionale;** • **Wp 248 (linee guida Gruppo Art. 29) n. 7:** - **valutazione circa lo status di vulnerabilità dell'interessato: i dati trattati riguardano soggetti vulnerabili (bambini, dipendenti, soggetti con patologie psichiatriche, richiedenti asilo, anziani e pazienti, etc);** • **Valutazioni ex Provv. Garante n. 467 del 11/10/2018 n.6:** - **Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);**

accountability del titolare/ TIA

DPIA correlate / versioning	**no**

Valutazione delle misure atte a garantire necessità e proporzionalità del trattamento (art. 35, paragrafo 7, lettera b)	
Finalità determinate, esplicite e legittime	diagnosi, cura e riabilitazione contenute nell'informative reperibile sul sito istituzionale del Titolare e presso le sue sedi
Liceità del trattamento (art. 6; art 9 GDPR e Art. 2-sexies D.lgs. 196/03)	Art. 9 par 2 lett. h) GDPR Art. 6 par 1 lett. c) GDPR; Art. 2-sexies D.lgs. 196/03 comma 1bis, comma 2 lett. t), u), v)
Adeguatezza, pertinenza e non eccedenza (art. 5, par. 1, lettera c));	garantita da policy (xx) interne, formazione privacy del personale e deontologia.
Esattezza e aggiornamento dei dati (art. 5, par. 1, lettera d))	garantita da policy interna (xx)
Limitazione della conservazione (Retention) (art. 5, par. 1, lettera e))	massimario di scarto, indicazioni al Responsabile dpa

accountability del titolare/ TIA

Valutazione delle misure atte a garantire i diritti degli interessati	
Informazioni fornite all'interessato (artt. 12, 13, 14)	informativa fornita sul sito istituzionale del Titolare e presso le sue sedi
Accesso (art.15); Portabilità dei dati (art. 20); Rettifica (art.16); Diritto all'oblio (art.17); Obbligo notifica (art. 19); Limitazione (art. 18); opposizione trattamento (art. 19, 21); **reclami (artt. 41, 43, 57);**	garantita da policy interna (xx) procedura e modulo per esercizio dei diritti dell'interessato reperibile sul sito istituzionale del Titolare e presso le sue sedi
Rapporti con i Responsabili del trattamento (art. 28)	DPA
Garanzie riguardanti trattamenti internazionali (capo V)	DPA + SCC
Consultazione preventiva (articolo 36)	no

accountability del titolare/ TIA

Gestione rischi per i diritti e le libertà degli interessati	
Risultanze complessive dell'Analisi del rischio	livello di rischio complessivo basso, riepilogo analisi dei rischi come riassunto qua sotto.
Fonti di rischio **(Es. Accesso illegittimo, modifica indesiderata, scomparsa dei dati)**	accesso illegittimo ai dati; modifica indesiderata dei dati; indisponibilità dei dati;
Minacce che potrebbero determinare accesso illegittimo, modifica indesiderata e scomparsa dei dati	catastrofi ambientali/agenti malevoli
Impatti potenziali per i diritti e le libertà degli interessati in casi di eventi avversi sui dati	danni per la salute dell'interessato/disagi nel compimento del percorso di cura, perdite economiche.
Misure previste per gestire i rischi **(art. 35, paragrafo 7, lettera d)**	policy del titolare, misure tecniche implementate da capitolato di gara nonché contenute nel DPA/TOM's del Titolare
Coinvolgimento delle parti interessate	
Parere del DPO sull'intero documento	nulla osta/favorevole
Parere degli interessati o loro rappresentanti	ritenuto non necessario
Esito finale della valutazione	nulla osta avvio del trattamento
Note	
Versioning DPIA	1.1.

2. Identificare lo strumento di trasferimento su cui si fa affidamento:

- considerato però che Alfa non compare nella Data Privacy Framework List,
- e considerate le caratteristiche del trattamento;
- il DPA sottoscritto con il Responsabile incorpora comunque, **per il primo anno di vigenza**, le SCC approvate mod 2 (transfer Controller to Processor) con riserva per il Responsabile del trattamento di aderire, medio tempore, alla Decisione di Adeguatezza del 10 luglio 2023.

accountability del titolare/ TIA

(estratto)

DECISIONE DI ESECUZIONE (UE) 2021/914 DELLA COMMISSIONE del 4 giugno 2021 relativa alle clausole contrattuali tipo
MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento
Allegato IA (elenco delle parti)

- Esportatore: Azienda Ospedaliera di Valle Grande;
- Indirizzo: via XYZ….;
- Nome qualifica e dati di contatto del referente: YYYY;
- Attività pertinenti ai dati traferiti a norma delle presenti clausole: troubleshooting di secondo livello su sistemi di trattamento dati automatizzati;
- Ruolo: Titolare;

accountability del titolare/ TIA

- Importatore: Ditta ALFA;
- Indirizzo: via zzzz, - USA;
- Nome qualifica e dati di contatto del referente: KKKK;
- Attività pertinenti ai dati traferiti a norma delle presenti clausole: troubleshooting di secondo livello su sistemi di trattamento dati automatizzati;
- Ruolo: Responsabile del Trattamento;

accountability del titolare/ TIA

Allegato IB (descrizione del trasferimento)

- Categorie di interessati: pazienti della AO di Valle Grande;
- Categorie di dati personali trasferiti: comuni e particolari che rivelano lo stato di salute;
- Dati sensibili trasferiti e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari: **indicate nell'allegato II**;

accountability del titolare/ TIA

- Frequenza del trasferimento: on demand;
- Natura del trattamento: medico diagnostico;
- finalità del trasferimento dei dati e dell'ulteriore trattamento: troubleshooting, interventi tecnici di secondo livello da remoto su sistemi oggetto della fornitura;
- Periodo di conservazione dei dati personali: indicati nel DPA, immediata cancellazione copie di back up dopo gli interventi;
- Per i trasferimenti a subresponsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento: subcontroller server spa, corr. in Luxemburg recapiti referente ….., gestione server Z;

accountability del titolare/ TIA

- Allegato IC (Autorità di Controllo competente): Garante per la Protezione dei Dati Personali – Roma Italy.
- Allegato II misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati: misure del DPA all. C.
- Allegato III elenco dei sub-responsabili del trattamento: all. B del DPA.

accountability del titolare/ TIA

3. Valutare se lo strumento di trasferimento invocato è efficace alla luce delle circostanze di trasferimento:

- Fisa section 702 (Legge sulla sorveglianza dei servizi segreti stranieri) consente alle intelligence statunitensi di raccogliere informazioni su persone fisiche situate al di fuori degli USA chiedendole ai fornitori di servizi di comunicazione elettronica. Tali attività sono subordinare alla previa approvazione della Foreign Intelligence Surveillance Court di Washington DC;

accountability del titolare/ TIA

- Executive Order (EO) 12333 autorizza le intelligence statunitensi (es. National Security Agency) a raccogliere informazioni personali riconducibili ad «intelligence straniere» transitate o accessibili via radio, filo, e altri mezzi elettromagnetici. Tale attività non si basa sull'assistenza obbligatoria dei fornitori di servizi di comunicazione elettronica, ma fa affidamento sullo sfruttamento delle vulnerabilità di tali infrastrutture;
- Cloud Act consente al Governo USA di accedere ai dati personali in cloud extra USA (anche tale attività è subordinata all'autorizzazione di un Tribunale indipendente USA).

• EO 1233 e Cloud Act vietano comunque la raccolta di dati in blocco e la sorveglianza di massa.

accountability del titolare/ TIA

Come tutti i soggetti che hanno sede negli USA e che intrattengono rapporti giuridici caratterizzati da un elevato livello di automazione digitale, anche Alfa è soggetta all'applicazione della predetta normativa tuttavia, viste le indicazioni in materia dell'EPBD, nonché quanto specificato nel White Paper del Dipartimento di Giustizia di Settembre 2020 «Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II», si osserva che:

- le informazioni trattate da Alfa quale Responsabile del trattamento e che si riferiscono a condizioni di salute di interessati UE sono scarsamente appetibili per le azioni intraprese dalle agenzie di intelligence statunitensi che probabilmente non saranno interessate a raccogliere tali dati.

accountability del titolare/ TIA

- infatti Alfa non ha mai ricevuto richieste di sicurezza nazionale ai sensi della predetta normativa (FISA section 702, EO 12333, Cloud Act).

4. Identificare le misure tecniche, contrattuali e organizzative applicate per proteggere i dati:

- i data center sono ubicati in UE;
- il Responsabile del trattamento, in applicazione di quanto previsto nel DPA + SCC, comunica annualmente un Trasparency Report sulle richieste governative di accesso ai dati. Il Responsabile è altresì obbligato ad esaminare ed eventualmente a contestare tali richieste laddove siano considerate illegali, nonché a contestare l'eventuale divieto alla comunicazione di accesso al titolare o a chiedere una deroga;

accountability del titolare/ TIA

- per limitare l'impatto, gli accessi di secondo livello sono abilitati on demand su specifica richiesta del personale del titolare, inoltre il DPA impone la immediata cancellazione delle copie di back up (cfr. DPA);
- sicurezza/certificazioni, trasferimenti successivi, privacy by design, formazione ecc. (cfr. DPA).

5. Valutazione finale:

- Alla luce delle informazioni contenute in questo documento e verificate da questo titolare, considerate anche l'esperienza maturata dal Responsabile in materia di richieste governative e le misure tecniche, contrattuali e organizzative implementate dallo stesso per proteggere i dati personali trattati per conto del titolare stesso, si ritiene che i rischi connessi al trasferimento e al trattamento dei dati personali europei negli Stati Uniti non influiscano sul rispetto degli obblighi previsti dalle SCC. Al momento non si ravvisa la necessità di adottare ulteriori misure supplementari.

6. Rivalutare a intervalli appropriati:

- se necessario, le parti si impegnano a riconsiderare i rischi connessi al trattamento e le misure implementate;
- le parti convengono di riesaminare lo strumento di trasferimento extrafrontaliero dei dati personali entro un anno dalla data odierna al fine di valutare l'utilizzo della recente Decisione di Adeguatezza adottata dalla Commissione il 10 luglio 2023 ed aggiornare la presente documentazione.

Letto Confermato Sottoscritto

Per il Titolare _____

Per il Responsabile del Trattamento _____