Centro di eccellenza Jean Monnet
"New Visions of the European Union's Role in Global Health" (EU4GH)

Ciclo di formazione professionale

Profili applicativi del diritto sanitario europeo

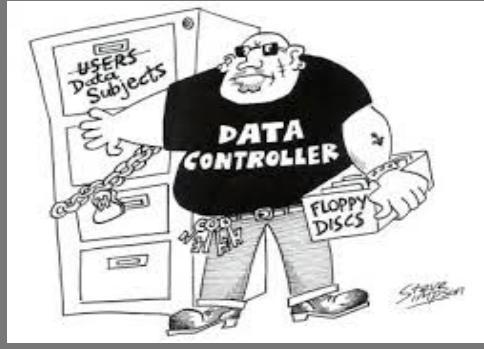
EU4GH Training Course

RIsk-based approach e sanità digitale: ipotesi applicative e circolazione dei modelli di responsabilità

Prof. avv. Giorgio Giannone Codiglione

Salerno, 13 giugno 2024

Risk-Based Approach e trattamento dei dati personali nel GDPR



Art. 4(1) - Nozione di dato personale : estesa a tutti i dati (anche quelli pseudonimi) che, anche a seguito di combinazione con altre informazioni, possano condurre all'identificazione di una persona fisica (cc.dd. trattamenti multipli).

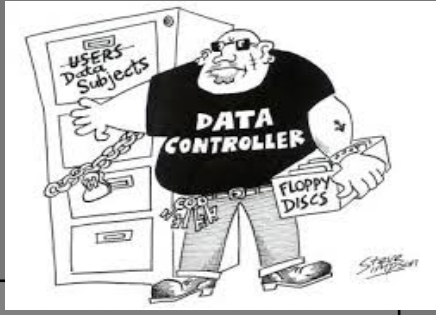
Art. 7 - Consenso: Il GDPR riafferma in maniera più incisiva il principio del consenso, affiancato ai doveri di informazione e trasparenza posti in capo al titolare o responsabile del trattamento. La disciplina è declinata in maniera analitica e puntuale anche con riguardo alla tutela di particolari figure soggettive, quali i minori (v. art. 8) e, ancora, con riferimento a particolari tipologie di trattamento dei dati.

Art. 6(4) – Trattamenti secondari:
In assenza di consenso dell'interessato o di altro atto legislativo che sancisca la liceità dell'attività, il titolare è tenuto a valutare se il trattamento sia astrattamente conforme ai principi di necessità e proporzionalità di cui all'art. 23 del Regolamento , con particolare riguardo agli scopi perseguiti dal trattamento principale.

Art. 35 – Valutazione d'impatto econsultazione preventiva: Nelle ipotesi di trattamento avente "un elevato rischio per i diritti e le libertà delle persone fisiche", il titolare è tenuto ad attuare una valutazione preventiva dell'impatto delle attività sulla protezione dei dati personali e, ove lo ritiene opportuno, consulta preventivamente l'autorità nazionale di garanzia al fine di ottenere l'autorizzazione per svolgere il trattamento.
- **Registro dei trattamenti**: obbligatorio + 250 dipendenti

EU4GH Training Course

Dal «pericolo» al «rischio»: correzione vs. prevenzione



- La **responsabilizzazione del titolare del trattamento** richiede l'**adozione proattiva** di misure idonee a garantire la promozione e la salvaguardia della protezione dei dati nel corso delle attività di trattamento.

- I titolari **sono responsabili per - e devono essere in grado di dimostrare - il rispetto della normativa in materia di protezione dei dati** nello svolgimento delle attività di trattamento, su richiesta delle persone interessate, del pubblico in generale e delle autorità di controllo.

- Il GDPR stabilisce nuovi obblighi in termini di responsabilizzazione che richiedono l'adozione di **significative misure di carattere tecnico e organizzativo** per dimostrare il rispetto del GDPR: la privacy "by design", la notifica delle violazioni della sicurezza alle autorità di controllo, la nomina di un rappresentante del titolare o del responsabile del trattamento stabilito al di fuori del territorio dell'Unione europea, nonché la conduzione di **valutazioni d'impatto sulla protezione dei dati per trattamenti a elevato rischio.**

EU4GH Training Course

Dal «pericolo» al «rischio»: danni civili vs. sanzioni amministrative

Art. 82(1), (2) e (3) – Diritto al risarcimento e responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento **risponde per il danno cagionato dal suo trattamento che violi il presente regolamento**. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Art. 15 Codice privacy previgente
Danni cagionati per effetto del trattamento

1. **Chiunque cagiona danno ad altri per effetto del trattamento di dati personali** è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Sanzioni amministrative

L'articolo 84 del GDPR prevede che gli Stati membri "stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie e adottano tutti i provvedimenti necessari per assicurarne l'applicazione [...]".

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (1)

a) Nozione di dato personale relativo alla salute e minimizzazione del trattamento

Tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Ad esempio:

- **informazioni raccolte nel corso della registrazione del paziente** al fine di ricevere servizi di assistenza sanitaria;

- un **numero, un simbolo o un elemento specifico** attribuito a una persona fisica per identificarla in modo univoco a fini sanitari;

- **informazioni risultanti da esami e controlli** effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici;

- **qualsiasi informazione** riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico *in vitro*.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (2)

a) Nozione di dato personale relativo alla salute e minimizzazione del trattamento

- In ossequio al **principio di minimizzazione**, **possono essere trattati solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati e/o ulteriormente elaborati**.

- Le categorie di dati scelti per il trattamento **devono essere necessarie al fine di conseguire la finalità generale** dichiarata delle attività di trattamento.

- Quanto alla durata del trattamento e alla relativa conservazione dei dati da parte del titolare (principi di adeguatezza e limitazione del trattamento), il GDPR specifica come **tali processi debbano essere limitati al tempo necessario** per il perseguimento delle finalità del trattamento.

- È possibile **fissare un termine** per la definitiva eliminazione delle informazioni o, ancora, ai fini dell'espletamento di una verifica periodica e di un'eventuale rettifica.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (3)

GPDP, n. 9784482/2022

Sul sito istituzionale di una ASL, nella sezione «Amministrazione trasparente», era possibile accedere a una pagina web in cui erano presenti due file intitolati: 1. «Registro degli accessi XX», contenente il «registro provvisorio richieste accesso agli atti» riferite a 1119 istanze, con specifica indicazione dei seguenti dati: numero di registro, data e numero di protocollo, oggetto, mittente, destinatario (url: https://...).

I documenti contenevano, nel campo oggetto e mittente, dati e informazioni personali, con specifica indicazione del nominativo del soggetto interessato o del proprio rappresentate legale (…). In un numero molto rilevante di casi erano contenuti anche dati relativi alla salute dei soggetti interessati, considerando che la tipologia di atti richiesti alla ASL, nella maggior parte degli accessi, era inerente a documentazione sanitaria (fra cui cartelle cliniche, accertamenti di invalidità, test, relazioni tecniche).

Il predetto trattamento è avvenuto in violazione:

1) del divieto di diffusione dei dati sulla salute dei soggetti interessati, previsto dall'art. 2-septies, comma 8, del Codice privacy (cfr. anche l'art. 9, parr. 1, 2 e 4, del GDPR);
2) del principio di «minimizzazione» dei dati, che non sono risultati «limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (ossia la trasparenza amministrativa), previsto dall'art. 5, par. 1, lett. c), del GDPR;
3) della disciplina statale in materia di trasparenza, per cui «Le pubbliche amministrazioni possono disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti che non hanno l'obbligo di pubblicare ai sensi del presente decreto o sulla base di specifica previsione di legge o regolamento, nel rispetto dei limiti indicati dall'articolo 5-bis, procedendo **alla indicazione in forma anonima dei dati personali eventualmente presenti**» (art. 7-bis, comma 2, del d. lgs. n. 33/2013).

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (4)

GPDP, n. 9857587/2022

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

L'Azienda Sanitaria ha pubblicato, sul sito web istituzionale, sezione albo pretorio, la determinazione n. XX del XX, contenente informazioni riguardanti il rapporto di lavoro tra l'Azienda Sanitaria e il reclamante, il procedimento disciplinare nei confronti dello stesso e indicazioni, compreso l'anno e il numero di registro generale, di un procedimento penale a carico del reclamante.

Sebbene, come sostenuto dall'Azienda Sanitaria, la determinazione in questione sia stata pubblicata nell'albo pretorio online **per soli 15 giorni**, l'Azienda non ha comprovato l'esistenza di una specifica norma di legge che obblighi l'ente a pubblicare l'integrale testo della determinazione di conferimento dell'incarico a un professionista per lo svolgimento della difesa in giudizio, non essendo sufficiente il richiamo fatto negli scritti difensivi al proprio regolamento per la gestione dell'albo pretorio, che non soddisfa, in ogni caso, i requisiti di una idonea base giuridica ai sensi dell'art. 2-ter, commi 1 e 3 del Codice (nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139).

Anche la presenza di uno specifico regime di pubblicità, non può comportare alcun automatismo rispetto alla diffusione online dei dati e informazioni personali, né una deroga ai principi in materia di protezione dei dati personali.

Nella determinazione oggetto della pubblicazione in **esame non avrebbe dovuto essere, quindi, riportato alcun dato personale del reclamante, ricorrendo, se del caso, alla tecnica degli "omissis" o ad altre misure di anonimizzazione dei dati**.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (5)

b) Consenso e limitazione della finalità

- Per le operazioni di trattamento di dati sulla salute necessari per la cura della salute degli interessati **non è richiesto il consenso degli interessati** (art. 9, par. 2 lett. h) e par. 3 del GDPR; GPDP 9 marzo 2019, doc. web 9091942).
- Le categorie particolari di dati personali che meritano una maggiore protezione **dovrebbero essere trattate soltanto per finalità connesse alla salute,** ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, (…).
- La finalità del trattamento dei dati deve essere chiaramente definita **prima** che il trattamento abbia inizio.
- **L'utilizzo ulteriore** dei dati per un'altra finalità richiede una base giuridica supplementare se la nuova finalità del trattamento è incompatibile con quella originaria.
- Ad esempio, il trasferimento di dati a soggetti terzi è una finalità nuova che richiede una base giuridica supplementare.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (6)

GPDP, n. 9819792/2022

L'Autorità ha ricevuto il reclamo della Sig.ra XX, in cui lamentava ripetuti accessi al proprio dossier sanitario aziendale da parte di un operatore sanitario operante presso una struttura di riabilitazione dell'Azienda Usl XXXXXX, ove la stessa ha dichiarato di non aver mai ricevuto assistenza sanitaria.

La reclamante inoltre ha rappresentato di aver negato il consenso al trattamento dei suoi dati personali attraverso il dossier sanitario aziendale.

Il dossier sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, costituisce **un trattamento di dati personali specifico e ulteriore** rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico. Come tale, quindi, si configura come un trattamento facoltativo.

Qualora l'interessato non manifesti il suo consenso al trattamento dei dati personali mediante il dossier sanitario il professionista che lo prende in cura avrà a disposizioni solo le informazioni rese in quel momento dallo stesso interessato (*es.* raccolta dell'anamnesi, delle informazioni relative all'esame della documentazione diagnostica prodotta) e quelle relative alle precedenti prestazioni erogate dallo stesso professionista.

I titolari devono porre particolare attenzione **nell'individuazione dei profili di autorizzazione e nella formazione dei soggetti abilitati**, dovendo essere limitato l'accesso al dossier al **solo personale sanitario che interviene nel processo di cura del paziente ed essere adottate modalità tecniche di autenticazione al dossier che rispecchino le casistiche di accesso a tale strumento proprie di ciascuna struttura sanitaria**. Il titolare del trattamento deve mettere in opera sistemi per il controllo degli accessi anche al database e per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti, attraverso l'utilizzo di indicatori di anomalie (c.d. alert) utili per orientare successivi interventi di audit.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (7)

c) Divieto di diffusione e principio di integrità e sicurezza

- Per i dati relativi alla salute è previsto – anche a tutela dei singoli e nel «rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona» (art. 1, comma 1, del Codice) – **un espresso divieto di diffusione**, ossia la possibilità di darne «conoscenza [...] a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione» (art. 2-septies, comma 8; art. 2-ter, comma 4, lett. b, del Codice privacy; art. 9 del GDPR, parr. 1, 2 e 4).
- Il medesimo divieto è peraltro richiamato dalla disciplina statale in materia di trasparenza, nella parte in cui prevede che «Restano fermi i limiti [...] alla diffusione dei dati idonei a rivelare lo stato di salute [...]» (art. 7-bis, comma 6, d. lgs. n. 33/2013).
- Il titolare del trattamento è comunque tenuto a rispettare i principi in materia di protezione dei dati, fra i quali quello di «integrità e riservatezza», secondo il quale i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza (...), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (art. 5, par. 1, lett. f) del GDPR).

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (8)

GPDP, n. 9861289/2023

Una ASL riceveva pec del XX con cui il paziente XXX ha comunicato che la copia di cartella clinica consegnata conteneva documentazione non riconducibile a sé stesso. Solo successivamente (in data XX), a restituzione di copia della cartella clinica, si è potuto verificare che la documentazione sanitaria riconducibile a soggetto diverso, riportava il nominativo di un soggetto terzo.

Le informazioni sullo stato di salute **possono essere comunicate unicamente all'interessato** e possano essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o previa delega scritta dell'interessato (art. 9 dal GDPR e art. 84 del Codice);

L'Azienda ha evidenziato che si è trattato di un caso isolato nel rilascio di copia della cartella clinica, **avvenuto a causa di un errore umano**.

Inoltre, ha ribadito che, appena venuta a conoscenza dell'accadimento da tale terzo destinatario ha chiesto a quest'ultimo, e ottenuto, la riconsegna dell'intera cartella clinica ricevuta, nonché la conferma del massimo riserbo in ordine alle informazioni eventualmente apprese e che nei giorni immediatamente successivi alla rilevazione dell'evento **ha provveduto ad aggiornare la procedura operativa relativa alle modalità di verifica della completezza della cartella clinica** e organizzato eventi formativi per il personale in materia di gestione della documentazione medica.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (9)

GPDP, n. 9832526/2022

In data 30 aprile, l'operatore che quel giorno si è occupato della trasmissione dei referti via PEC ha caricato tutti i referti da inviare nella cartella *spool*. Il referto del sig. XX e della signora XX erano uno di seguito all'altro. Per mero errore materiale, è stato allegato il referto sbagliato".

L'assistito ha la possibilità di richiedere, ai sensi degli artt. 38 e 65 del CAD, la trasmissione del referto a mezzo PEC. Il personale amministrativo giornalmente archivia in apposito raccoglitore la stampa delle richieste di trasmissione telematica del referto, annotando su ciascuna il rispettivo codice alfanumerico univoco generato in fase di accettazione del campione. Il personale verifica quali referti per l'utenza esterna sono stati firmati e sono dunque pronti per l'invio. I referti disponibili per la consegna vengono "scaricati" da Armonia e salvati - identificati da nome/cognome paziente e id referto - in una cartella Spool.

L'Azienda - pur **nella rappresentata osservanza del principio di segregazione dei compiti**, nel **dichiarato rispetto della separazione (fisica o logica) dei dati personali e affidamento di diversi profili di autorizzazione per l'accesso agli stessi** - ha determinato, per le attività che svolge per conto di XXXXXX in qualità di responsabile del trattamento ("esami istologici su biopsie mammarie, colorettali, cervicali, su polipi del colon retto e su lesioni cutanee"), una comunicazione di dati sulla salute di una paziente di XXXXXXX medesimo a soggetto non legittimato a riceverli.

Al riguardo l'Azienda, al fine di **minimizzare il rischio** di futuri accadimenti analoghi ha impartito indicazioni agli operatori di "scaricare nella cartella di servizio un solo referto per volta, eliminandolo dopo aver effettuato la trasmissione", nonché avviato un confronto con i tecnici informatici di ESTAR per migliorare le attuali misure di segregazione fisica o logica dei dati personali.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (10)

GPDP, n. 10001279/2024

La Asl XXX è stata sanzionata per 75.000 per non aver configurato correttamente le modalità di accesso al dossier sanitario elettronico (Dse).
L'Autorità si è attivata a seguito di alcuni reclami e segnalazioni che lamentavano il trattamento illecito di dati personali effettuato tramite il sistema di archiviazione e refertazione delle prestazioni erogate dall'azienda sanitaria. In particolare, erano stati segnalati ripetuti accessi al Dse da parte di personale sanitario non coinvolto nel processo di cura dei pazienti. In un caso, una professionista della Asl era infatti riuscita a visionare gli esami di laboratorio dell'ex marito a sua insaputa pur essendo quest'ultimo non in cura dalla stessa.

Dalle verifiche effettuate è emerso che il sistema di gestione del Dse consentiva agli operatori sanitari di inserire manualmente, mediante autocertificazione, la motivazione per cui si rendeva necessario l'accesso al dossier sanitario. L'accesso al documento era inoltre consentito, per impostazione predefinita, ad una ampia lista di figure professionali che niente avevano a che fare con il percorso di cura dei pazienti, compreso il personale amministrativo.

Il tutto in violazione di quanto stabilito con le "*Linee guida in materia di Dossier sanitario*" del giugno 2015, con cui l'Autorità ha stabilito che "*il titolare del trattamento deve porre particolare attenzione nell'individuazione dei profili di autorizzazione, adottando modalità tecniche di autenticazione al dossier che rispecchino le casistiche di accesso proprie di ciascuna struttura*" garantendo che l'accesso al dossier sia limitato al solo personale sanitario che interviene nel tempo nel processo di cura del paziente.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (11)

d) La trasparenza nel trattamento: informativa vs. informazione

- L'interessato **dovrebbe sempre ricevere le informazioni relative al trattamento di dati personali** che lo riguardano di cui all'art. 13 del GDPR al momento della raccolta presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso e in una forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (cons. 39, 58 e art. 12 del GDPR).
- Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali.
- Tra le informazioni da rendere agli interessati **rileva, in particolare, la base giuridica del trattamento** (artt. 13, par. 1, lett. c) e 14, par. 1 lett. c) del GDPR).
- Rileva inoltre l'indicazione del **periodo di conservazione**, nel rispetto di stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.

EU4CH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (12)

GPDP, n. 9742959/2022

I modelli recanti le informazioni da rendere agli interessati, pubblicati sul sito internet dell'Azienda XXXX sono risultati non conformi al quadro normativo in materia di protezione dei dati personali, in quanto:

- risultavano indicate **molteplici finalità di trattamento**, quali quelle di cura, amministrative e di ricerca scientifica, ma non sempre erano chiaramente indicate le relative basi giuridiche, che laddove richiamate risultavano comunque erronee o contraddittorie;
- indicavano nel consenso la condizione di liceità dei trattamenti necessari per finalità di cura:
- pur citandosi correttamente nella parte introduttiva l'art. 9, par. 2, lett. h) del GDPR (finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali), **come condizione di liceità per il trattamento dei dati necessari per finalità di cura,** veniva erroneamente ribadita l'indispensabilità del consenso degli interessati per poter accedere alle cure**;**
- **non sempre era indicato il periodo di conservazione** dei dati personali o erano indicati solo i tempi di conservazione delle cartelle cliniche);
- era erroneamente indicato tra i diritti dell'interessato il diritto alla portabilità dei dati (art. 20 del GDPR);
- erano indicate tre differenti finalità perseguite dal titolare del trattamento (di cura, amministrative e di ricerca scientifica) e riportata la base giuridica relativa solo ad una di esse (la finalità di cura della salute), e non si comprendeva a quale delle tre finalità perseguite si riferiva il tempo di conservazione ivi indicato;
- era riportato l'interesse legittimo quale base giuridica del trattamento.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (13)

e) Corretta gestione delle richieste di esercizio dei diritti dell'interessato

- Gli artt. 12 e ss. del GDPR in materia di "diritti dell'interessato", prevedono il diritto di quest'ultimo di ottenere dal titolare del trattamento quanto richiesto ai sensi degli artt. da 15 a 22, **senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta.**

- Se **non ottempera** alla richiesta dell'interessato, il titolare del trattamento **informa quest'ultimo senza ritardo, al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale** (art. 12, paragrafo 4, del Regolamento).

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (14)

GPDP, n. 9853446/2023

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

L'Azienda sanitaria, a fronte della richiesta avanzata dall'interessata in data XX, non ha fornito risposta, né ha rappresentato idonei motivi per giustificare tale inottemperanza, provvedendo, in tal senso, solo a seguito dell'invito di questa Autorità, del XX, formulato nell'ambito del procedimento relativo al reclamo. L'Azienda sanitaria, in data XX, prima che l'interessata esercitasse i diritti previsti dal GDPR, aveva, comunque, provveduto alla cancellazione del dato non corretto risultante dal certificato vaccinale anti Covid-19 relativo a quest'ultima.

L'Azienda ha dichiarato che i "(...) motivi del mancato riscontro scritto sono da rinvenirsi nell'emergenza pandemica coronavirus che aveva determinato carichi di lavoro straordinari ed imprevisti (...) (e) ostacolato l'adempimento nei tempi previsti dalla procedura adottata da quest'Azienda per l'esercizio dei diritti degli interessati, pubblicata sul sito istituzionale nell'apposita sezione "privacy"

Non avendo la struttura sanitaria fornito risposta a fronte della richiesta di accesso ai propri dati personali avanzata - ai sensi dell'art. 15 del GDPR - dall'interessata in data XX, né rappresentato idonei motivi per giustificare tale inottemperanza, provvedendo, in tal senso, solo a seguito dell'invito di questa Autorità, del XX, formulato nell'ambito del procedimento relativo al sopra citato reclamo, si confermano le valutazioni preliminari dell'Ufficio e si accerta la violazione dell'art. 12, par. 3, in relazione all'art. 15 del GDPR

La ASL XXX ha successivamente adottato **misure tecniche ed organizzative adeguate** per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati nei termini di legge, approvando la "**Procedura di gestione dei diritti degli interessati - Regolamento UE 2016/679**".

La suddetta procedura è stata debitamente diffusa a tutto il personale ed è stata pubblicata sul sito istituzionale aziendale nella sezione "privacy"; inoltre tutte le strutture aziendali sono state sollecitate ad attenersi scrupolosamente alle procedure aziendali in materia di protezione di dati personali".

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (15)

f) Trattamenti «secondari», «altamente rischiosi» e valutazione d'impatto

- Art. 6(4) del GDPR

Trattamenti secondari: in assenza di consenso dell'interessato o di altro atto legislativo che sancisca la liceità dell'attività, **il titolare è tenuto a valutare se il trattamento sia astrattamente conforme ai principi di necessità e proporzionalità di cui all'art. 23 del GDPR.**

- Tale vaglio preventivo deve essere svolto **tenendo in considerazione ogni possibile nesso sussistente tra le diverse finalità,** il contesto in cui i dati personali sono stati raccolti, la loro natura, le possibili conseguenze dell'ulteriore trattamento e l'esistenza di garanzie adeguate volte a minimizzare i rischi ad esso sottesi, quali la cifratura o la pseudonimizzazione.

- Nelle ipotesi di trattamento avente "*un elevato rischio per i diritti e le libertà delle persone fisiche*", il titolare è tenuto ad attuare **una valutazione preventiva dell'impatto delle attività sulla protezione dei dati personali** e, ove lo ritiene opportuno, consulta preventivamente l'autorità nazionale di garanzia al fine di ottenere l'autorizzazione per svolgere il trattamento.

EU4CH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (16)

f) Trattamenti «secondari», «altamente rischiosi» e valutazione d'impatto

- **Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto (**GPDP, 11 ottobre 2018):

- **1)** Trattamenti valutativi o di ***scoring*** su larga scala, nonché trattamenti che comportano la **profilazione** degli interessati nonché lo svolgimento di **attività predittive** effettuate anche online o attraverso app, relativi ad "*aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gliinteressi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*"; (…)

- 6) Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo); (…)

- 10) Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse; (…)

- 12) Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (17)

f) Trattamenti «secondari», «altamente rischiosi» e valutazione d'impatto

- Il titolare del trattamento, coadiuvato dal DPO, analizza i punti di criticità del trattamento e redige un documento di sintesi con la descrizione delle operazioni di trattamento e delle finalità in rapporto ai principi di necessità e proporzionalità e ai rischi per i diritti e le libertà dell'interessato, nonché elenca le misure previste per contrastarne l'occorrenza sul piano della sicurezza, della protezione degli interessi dei soggetti coinvolti e della generale conformità al GDPR.

- Ove gli esiti della valutazione d'impatto conducano all'individuazione di un rischio elevato in assenza dell'adozione di misure idonee ad attenuarne gli effetti pregiudizievoli (art. 36 n. 1), i risultati della valutazione d'impatto sono posti al vaglio preventivo dell'autorità di controllo. Quest'ultima, nel caso di trattamento illecito o non adeguatamente vagliato sul piano del rischio, ha l'onere di produrre entro otto settimane dalla ricezione della richiesta (prorogabile per altre sei previa informativa al titolare) un **parere scritto**, esercitando altresì i poteri investigativi, correttivi, autorizzativi e consultivi di cui all'art. 58. Nell'analizzare i risultati della valutazione svolta dal titolare, l'autorità tiene in particolare considerazione il rispetto dei codici di condotta (art. 36, n. 8).

EU4CH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (18)

GPDP, n. 9845156/2022

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

L'iniziativa ha previsto l'estrazione di dati sulla salute degli assistiti dal Datawarehouse dell'Azienda per il tramite della Società XXXXXXX, nominata Responsabile del trattamento, attraverso l'utilizzo di un algoritmo fornito dalla Agenzia regionale XXXXXXX.

Tale attività prevede una stratificazione degli assistiti del Servizio sanitario regionale in base alle informazioni relative allo stato di salute individuale, per la relativa collocazione in classi di rischio sanitario, al fine di individuare modelli assistenziali volti alla promozione attiva di interventi sanitari che mirano a una precoce presa in carico degli stessi.

Con specifico riferimento alla circostanza che sarebbero stati estratti dalla società XXX solo i dati di coloro che hanno prestato il consenso alla consultazione del FSE, tenuto conto delle specifiche finalità perseguite che non comprendono quelle di medicina di iniziativa, si rappresenta che il consenso manifestato per i trattamenti effettuati attraverso il FSE non può considerarsi un idoneo presupposto di liceità. Tali trattamenti **devono essere infatti considerati ulteriori e autonomi rispetto a quelli strettamente necessari alle ordinarie attività di cura e prevenzione** (art. 9, par. 2 lett. h) del GDPR), **e quindi effettuabili solo sulla base dello specifico consenso informato dell'interessato** (art. 9, par. 2 lett. a) del GDPR).

I trattamenti effettuati dall'Azienda hanno riguardato dati relativi alla salute di un numero elevato di soggetti vulnerabili, non può pertanto condividersi la posizione del titolare del trattamento in base alla quale una preventiva valutazione di impatto, ai sensi dell'art. 35 del GDPR, non sarebbe stata necessaria,

Per il trattamento in esame, ricorrono certamente due dei criteri indicati dal Comitato Europeo per la protezione dei dati per individuare i casi in cui un trattamento debba formare oggetto di una valutazione di impatto. In particolare, si fa riferimento ai seguenti criteri: **trattamento di "dati sensibili o aventi carattere altamente personale" e di "dati relativi ad interessati vulnerabili" tra i quali si annoverano i malati**.

EU4GH Training Course

Case-study: approccio basato sul rischio e trattamento dei dati personali relativi alla salute (19)

GPDP, n. 9988614/2024

L'azienda XXX ha presentato un'istanza di consultazione preventiva sullo studio «IA per la definizione di nuove *signature* e modelli per la personalizzazione delle strategie di preservazione d'organo del cancro XXX» per cui i dati **raccolti** dovrebbero essere trattati attraverso logiche algoritmiche, con strumenti di intelligenza artificiale e con logiche predittive basate su sistemi di machine learning.

L'art. 22 del GDPR stabilisce che "*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*", ciò a meno che, con riferimento al trattamento delle particolari categorie di dati, esso si basi sul **consenso degli interessati** ovvero sia svolto sulla base di uno specifico presupposto normativo per motivi di interesse pubblico rilevante e "*siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato*".

a) **Principio di conoscibilità:** ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino ed in questo caso a ricevere informazioni significative sulla logica

b) **Principio di non esclusività della decisione algoritmica:** deve comunque esistere nel processo decisionale un intervento umano capace di controllare, validare ovvero smentire la decisione automatica (c.d. *human in the l*oop);

c) **Principio di non discriminazione algoritmica:** è opportuno che il titolare utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche.

EU4GH Training Course

Circolazione dei modelli e trattamento di dati sanitari svolto da sistemi di IA: GDPR *vs*. IA Act (1)

- Generare contenuti, fare previsioni o adottare decisioni in maniera automatica, come fanno i sistemi di IA, per mezzo di tecniche di apprendimento automatico o regole di inferenza logica e probabilistica è cosa ben diversa rispetto alle modalità con cui queste stesse attività sono svolte dagli esseri umani attraverso il ragionamento creativo o teorico, nella piena consapevolezza della responsabilità delle relative conseguenze.

- Se da una parte, l'IA amplierà significativamente la quantità di previsioni che si possono fare in molti ambiti – a cominciare dalle correlazioni quantificabili tra i dati-, dall'altra affidare solo alle macchine il compito di prendere decisioni sulla base di dati comporterà rischi per i diritti e le libertà delle persone che incideranno sulla loro vita privata e potrebbero nuocere a categorie sociali o persino a intere società.

- Nel parere congiunto del Comitato europeo per la protezione dei dati e il Garante europeo, n. 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale, del 21 aprile 2021), nel quale viene accolto con favore **l'approccio basato sul ris**chio su cui si fonda la proposta.

- Nel suddetto parere congiunto n. 5/2021 si evidenzia che i rischi per i diritti e le libertà fondamentali degli interessati derivanti dall'utilizzo di tali strumenti e le implicazioni per la protezione dei dati personali, sono molto rilevanti e viene sottolineato come tra i sistemi di IA ad alto rischio dovrebbero essere contemplati anche quelli utilizzati nell'ambito della ricerca medica.

EU4GH Training Course

Circolazione dei modelli e trattamento di dati sanitari svolto da sistemi di IA: GDPR *vs.* IA Act (2)

- Considerando n. 1) AI Act: «(…) *promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ("Carta"), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione*. (…)».

- Considerando n. 25 dell'AI Act: «*Il presente regolamento dovrebbe sostenere l'innovazione, rispettare la libertà della scienza e non dovrebbe pregiudicare le attività di ricerca e sviluppo. È pertanto necessario escludere dal suo ambito di applicazione i sistemi e i modelli di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici. È inoltre necessario garantire che il regolamento non incida altrimenti sulle attività scientifiche di ricerca e sviluppo relative ai sistemi o modelli di IA prima dell'immissione sul mercato o della messa in servizio. Per quanto riguarda le attività di ricerca, prova e sviluppo orientate ai prodotti relative ai sistemi o modelli di IA, le disposizioni del presente regolamento non dovrebbero nemmeno applicarsi prima che tali sistemi e modelli siano messi in servizio o immessi sul mercato*. (…) *In ogni caso, qualsiasi attività di ricerca e sviluppo dovrebbe essere svolta conformemente alle norme etiche e professionali riconosciute nell'ambito della ricerca scientifica e dovrebbe essere condotta conformemente al diritto dell'Unione applicabile*».

EU4CH Training Course

Circolazione dei modelli e trattamento di dati sanitari svolto da sistemi di IA: GDPR *vs*. IA Act (3)

- Considerando n. 26) AI Act: «*AI fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di IA inaccettabili, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA*».

- Considerando n. 47 dell'AI Act: «*I sistemi di IA potrebbero avere un impatto negativo sulla salute e sulla sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di sicurezza dei prodotti. Coerentemente con gli obiettivi della normativa di armonizzazione dell'Unione di agevolare la libera circolazione dei prodotti nel mercato interno e di garantire che solo prodotti sicuri e comunque conformi possano essere immessi sul mercato, è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati. Ad esempio, i robot sempre più autonomi, sia nel contesto della produzione sia in quello della cura e dell'assistenza alle persone, dovrebbero essere in misura di operare e svolgere le loro funzioni in condizioni di sicurezza in ambienti complessi. Analogamente, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati*».

EU4GH Training Course

Circolazione dei modelli e trattamento di dati sanitari svolto da sistemi di IA: GDPR *vs*. IA Act (4)

- Centralità del **concetto di sorveglianza (o supervisione) umana** (cfr. art. 14 AI Act): «*I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso* (…)».

- L'effettiva importanza degli esseri umani nelle decisioni algoritmiche dovrebbe fondarsi su **una supervisione altamente qualificata e sulla liceità del trattamento**, al fine di assicurare il rispetto del diritto di non essere assoggettato a una decisione basata esclusivamente su un trattamento automatizzato. (si v. anche il «D*ecalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale*» adottato dal GPDP il 10 ottobre 2023 (doc. web n.9938038)).

- La disciplina in materia di protezione dei dati personali non trova invece applicazione in relazione ai dati anonimi. Un processo di anonimizzazione non può definirsi effettivamente tale qualora non risulti idoneo ad impedire che chiunque utilizzi tali dati, in combinazione con i mezzi "ragionevolmente disponibili", possa: a) isolare una persona in un gruppo (*single-out*); b) collegare un dato anonimizzato a dati riferibili a una persona presenti in un distinto insieme di dati (*linkability*); c) dedurre nuove informazioni riferibili a una persona da un dato anonimizzato (i*nference*).

EU4GH Training Course

UNIVERSITÀ DEGLI STUDI DI SALERNO
Facoltà di Scienze Giuridiche (Scuola di Giurisprudenza)

Grazie per l'attenzione!

ggiannonecodiglione@unisa.it

EU4GH Training Course