ALLEGATO C: ISTRUZIONI OPERATIVE

Requisiti di sicurezza, ai sensi del Regolamento Europeo 679/2016 (Regolamento Generale per la Protezione Dati -GDPR), dei dispositivi medici/software/servizi che trattano dati personali

Il presente documento è redatto ai sensi degli Artt. 24, 25 e 32 del GDPR 2016/679.

Princìpi

Il nuovo Regolamento Europeo 2016/679 (GDPR) ha introdotto un innovativo approccio **sostanziale** alla materia introducendo il principio dell'**Accountability.**

Tale principio è conosciuto meglio come principio di "responsabilizzazione" e prevede che chiunque tratti dati personali in qualità di Titolare, Responsabile o Delegato, debba adottare e dimostrare di aver adottato tutte le misure di sicurezza che **egli stesso** abbia valutato necessarie al fine di proteggere adeguatamente i dati personali trattati.

Ciò comporta una doppia responsabilità, tanto per la valutazione quanto per l'applicazione delle misure.

Quanto premesso cristallizza le evidenti responsabilità in capo all'A.O.U. Policlinico Consorziale di Bari in relazione alla protezione dei dati personali.

Pertanto, qualsiasi nuova acquisizione di beni, dispositivi, servizi, software, ecc. (di seguito "gli Strumenti") che trattano dati personali, dovrà rispettare, **fin dalla progettazione** i requisiti previsti dalla normativa vigente in tema di protezione dei dati (c.d. **Privacy by Design**).

Ruoli nel GDPR

Nel rispetto del principio di accountability, un'altra azione fondamentale consiste nell'individuare **ruoli e responsabilità** nel nuovo trattamento. I ruoli previsti dal GDPR 2016/679 sono i seguenti:

- **Titolare** (l'A.O.U. Policlinico, e per essa il legale rappresentante).
- **Titolare autonomo** (questo ruolo solitamente è assunto da soggetti coinvolti in sperimentazioni, ricerche scientifiche, ecc. per il trattamento dei dati pseudonimizzati) (*in caso di utilizzo di dati personali in chiaro, ed acquisiti dal Policlinico, non è opportuno utilizzare tale ruolo*).
- **Contitolare** (si utilizza quando due titolari determinano congiuntamente le finalità e i mezzi per un trattamento dei dati personali) *(è necessaria una valutazione ad hoc prima di definire tale ruolo).*

- **Responsabile** (si utilizza quando l'A.O.U. Policlinico affida, ad una società o a una ditta individuale, una commessa che riguardi, direttamente o indirettamente il trattamento dei dati personali). *(Per esempio non è necessario affidare il ruolo di responsabile nel caso di fornitura di carta, penne, ecc. mentre è obbligatorio quando il fornitore viene a contatto direttamente o indirettamente con i dati personali trattati dal Policlinico sia dei pazienti che dei dipendenti).*
- **Responsabile con compiti di Amministratore di Sistema** (Questo ruolo deve essere attribuito ai fornitori di servizi, di apparecchiature informatiche, di software, di diagnostica per immagini e tutti i dispositivi con i quali e nei quali possono essere memorizzati e trattati i dati personali dei pazienti, dei dipendenti e di tutti gli interessati. *(Per esempio fornitura e manutenzione di software, server, ecografi, TAC, ecc.).*
- **Delegati interni**: Questo ruolo è affidato ai Direttori delle UU.OO.CC. Amministrative, Sanitarie e Tecniche, i quali hanno la responsabilità di far sì che nella propria realtà vengano rispettate le istruzioni impartite dal Titolare del trattamento (A.O.U. Policlinico – Direttore Generale) e vengano applicate le misure organizzative necessarie nel rispetto della normativa vigente.
- **Delegato con funzioni di Amministratore di sistema**, coincide con la figura del Responsabile dell'Ufficio ICT.
- **Soggetti autorizzati** : Sono tutti coloro che trattano dati in azienda, dipendenti ospedalieri, dipendenti universitari in convenzione, specializzandi, studenti, medici frequentanti, ecc.
- **Soggetti autorizzati con funzioni di amministratore di sistema**: rientrano in tale figura i soggetti che svolgono la propria attività lavorativa presso l'Ufficio ICT ed ai quali è stato affidato il compito di espletare delle attività sui sistemi informativi aziendali sotto la supervisione del Delegato con funzioni di Amministratore di sistema.

Misure di sicurezza dei dispositivi, software, ecc.

Nel rispetto del principio della **privacy by design** e dell'**accountability** è imprescindibile che la controparte (fornitore, soggetto convenzionato, ecc.) fornisca preventivamente tutte le informazioni necessarie sul trattamento dei dati personali.

Quanto sopra, è necessario affinché si possano valutare le misure di sicurezza tecniche ed organizzative a protezione dei dati contenuti nello Strumento e trattati con esso per effettuare, quando necessario, l'obbligatorio calcolo preventivo del livello di rischio per i diritti e le libertà degli interessati ai quali si riferiscono i dati trattati.

Obblighi del fornitore

Il fornitore, il soggetto convenzionato o comunque la controparte dovrà comunicare al Policlinico:

1. le misure di sicurezza adottate
    a. la valutazione dei rischi effettuata
    b. la valutazione delle vulnerabilità del dispositivo, software, ecc.
2. la certificazione che l'oggetto della fornitura sia adeguato al GDPR
3. la descrizione del ciclo di vita dei dati (dall'acquisizione, alla memorizzazione fino alla distruzione)
4. la descrizione completa del trattamento dei dati indicando quanto previsto dall'Art. 30 del GDPR, quali:
    a. la denominazione del trattamento da effettuare attraverso lo "strumento" (ad esempio: gestione sanitaria dei pazienti);
    b. la finalità del trattamento (ad esempio: finalità di cura);
    c. le categorie di soggetti interessati (ad esempio: pazienti, dipendenti, ecc.);
    d. le categorie di dati personali trattati (ad esempio: dati di contatto, categorie particolari di dati);
    e. le categorie di destinatari a cui i dati possono o devono essere comunicati attraverso l'utilizzo dello Strumento (ad esempio: subresponsabili esterni e/o Enti previsti dalla legge);
    f. i Paesi stranieri verso cui i dati potrebbero essere trasferiti (nel caso i dati fossero memorizzati in cloud o per esempio si utilizzi un portale web del fornitore situato al di fuori dell'Unione Europea);
    g. le garanzie adottate a tutela del trasferimento internazionale dei dati personali (ad esempio: Clausole contrattuali standard, Privacy Shield, Binding Corporate Rules));
    h. il periodo di conservazione dei dati (ad esempio: 10 anni o comunque per il tempo necessario a tutelare i diritti legali del titolare);
    i. le misure di sicurezza fisiche, organizzative e tecniche adottate per la protezione dei dati;
    j. le misure tecniche adottate in caso di trasmissione in rete delle informazioni;
    k. la fonte dei dati personali (ad esempio: se conferiti dall'interessato o acquisiti da fonti esterne e/o da terzi);
    l. la necessità o meno di una valutazione d'impatto sulla protezione dei dati.

Esempi non esaustivi di misure di sicurezza

Con l'introduzione del principio dell'accountability, il GDPR ha responsabilizzato i titolari ed i suoi delegati all'adozione delle misure di sicurezza adeguate, ragion per cui non è possibile disporre di un insieme di misure di sicurezza che possano essere utilizzare a protezione di tutti i trattamenti.

Il nuovo paradigma prevede una valutazione caso per caso ed una implementazione delle misure di sicurezza ad hoc, strettamente correlate con la tipologia dei dati trattati e delle potenziali conseguenze sui diritti e le libertà dell'interessato.

Di seguito si individuano, **a titolo esemplificativo e non esaustivo**, alcune tipologie di informazioni da acquisire al fine di individuare il livello di rischio e le misure implementate:

- Descrizione del trattamento effettuato tramite lo Strumento, ecc. (ad es. se lo Strumento possa visualizzare, trasmettere e gestire dati personali in rete, quali tipi di dati tratti, etc)
- Tipologia di memorizzazione del dispositivo/software
- Misure di protezione per la trasmissione dei dati personali
- Misure a protezione da accessi non autorizzati
- Monitoraggio dell'utilizzo del dispositivo (log)
- Gestione dei profili di Autorizzazione Autenticazione
- Aggiornamenti di sicurezza
- Capacità del dispositivo/software di de-identificare i dati (pseudonimizzazione e anonimizzazione)
- Accesso in emergenza al dispositivo

Valutazione di Impatto

In funzione delle informazioni acquisite, il Titolare del Trattamento, ha l'obbligo di effettuare una valutazione di impatto, previo consulto con il Responsabile della Protezione Dati (Art. 35 GDPR), al fine di determinare il livello di rischio del trattamento e valutare l'opportunità di effettuare o meno il trattamento, qualora il tipo di trattamento presenti un rischio elevato per i diritti e le libertà degli individui.

Laddove si riscontri un livello residuo elevato di rischio, ai sensi dell'Art. 36 del GDPR, il Titolare deve inviare una consultazione preventiva all'Autorità di Controllo.

Responsabilità dei Dirigenti/Delegati

E' OBBLIGATORIO per tutti coloro i quali in Azienda predispongano gare, acquisizioni, convenzioni, prove dimostrative di dispositivi e servizi che vedono coinvolti i dati personali,

individuare il ruolo da attribuire al fornitore e verificare che quest'ultimo abbia adempiuto agli obblighi previsti dalla normativa vigente.

Si rammenta che l'affidamento di una fornitura ad un soggetto non conforme alla normativa vigente, in tema di protezione dati personali, espone l'A.O.U. Policlinico a pesantissime sanzioni per la mancata vigilanza.

È pertanto necessario acquisire dal fornitore, attraverso gli **ALLEGATI A e B** una dichiarazione che attesti la sua conformità alle disposizioni normative in tema di protezione dei dati personali oltre che tutte le informazioni utili nel rispetto del principio della privacy by design.

Coinvolgimento del Responsabile Protezione Dati

Ai sensi dell'Art. 38 del GDPR è obbligatorio il coinvolgimento del Responsabile della Protezione Dati in tutte le questioni relative alla protezione dei dati personali.

RIFERIMENTI NORMATIVI

Art. 24: **Responsabilità del titolare del trattamento (Accountability)**

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Art. 25: **Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita. (Privacy by Design e by Default)**

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative

adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Art. 32: Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

   a) la pseudonimizzazione e la cifratura dei dati personali;

   b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

   c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

   d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 38: Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.