LEGENDA SPECIFICHE:

A seguito degli elementi raccolti , potrà essere necessario espletare da parte di codesta struttura una DPIA per valutare i rischi privacy correlati, qualora non già e

Processo di trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Area interessata: la struttura organizzativa che gestisce il trattamento

Finalità del trattamento (sintetica): descrizione delle finalità per le quali si effettua il trattamento (es. normativa di riferimento, rapporto contrattuale di riferimento, diagnosi e cura, etc.)

Descrizione dettagliata del processo di trattamento:

es. chi fa cosa, chi vede cosa

Deve essere analizzato singolarmente ad esempio il trattamento correlato ad uno specifico rapporto convenzionale/contrattuale/derivante da protocollo d'intesa, in quanto abbia una sua peculiarità di gestione del flusso dei dati tra le parti contraenti e/o i soggetti coinvolti nell'espletamento delle attività sanitarie e non , che ne sono oggetto e/o interessati alle stesse.
L'analisi del flusso dati deve pertanto essere effettuata coinvolgendo gli operatori che concretamente lo gestiscono quale presupposto indispensabile alla corretta identificazione del trattamento.

Precisare se il trattamento è effettuato quale:

titolare («titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri)

o quale **contitolare** (Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati, anche ai

o quale **responsabile esterno** (Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, che è diverso da ASL3)?

Precisare in quale dei suddetti ruoli rientra il trattamento.

Si ricorda che sia il Titolare che il Contitolare che il responsabile esterno devono precisare in un loro registro dei trattamenti per ogni trattamento il ruolo ricoperto. Si ricorda in particolare che ex art.30.2 del Regolamento UE 2016/679 il responsabile esterno deve registrare i trattamenti effettuati per conto di uno o più titolari in un proprio registro specifico secondo il format disponibile sul sito intarnet aziendale. Ad es. se il trattamento correlato ad uno specifico rapporto convenzionale/contrattuale/derivante da protocollo d'intesa è svolto a favore di un ente diverso da ASL 3(es. altra azienda del SSR, altro ente pubblico o privato) perchè detto ente terzo fruisce di una prestazione , anche sanitaria (alla quale il trattamento dati è correlato), erogata da una struttura / operatore di ASL3, gli operatori di detta struttura di ASL3 /l'operatore di ASL3 opereranno ai fini privacy quale responsabile esterno designato dall'ente terzo ed il direttore della struttura di loro afferenza in ASL3 dovrà registrare il trattamento dati di cui trattasi nello specifico registro del responsabile esterno sopra

Modalità trattamento elettronico:

Indicando i profili di accesso (cioè i diversi gradi di visibilità, inserimento dati, verifica dati, controllo dati etc.in relazione al ruolo ricoperto nel trattamento) di eventuali applicativi utilizzati per il trattamento; l'ubicazione di eventuali banche dati, precisando se in cloud e se all'interno dell'UE o all'esterno.

Si ricorda che detta precisazione va effettuata valutando, in caso di utilizzazione di responsabile esterno per il trattamento, anche analoghe informazioni riguardanti l'attività dello stesso

Modalità di trattamento cartaceo: indicare se si e descrivere modalità di raccolta ed archiviazione, responsabilità della stessa, modalità di reperimento della documentazione.

Si ricorda che detta precisazione va effettuata valutando, in caso di utilizzazione di responsabile esterno per il trattamento, anche analoghe informazioni riguardanti l'attività dello stesso

Base giuridica del trattamento: Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità laddove previsto; b)il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (indicare la fonte normativa dell'obbligo); d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (indicare la fonte normativa).
Si ricorda che il trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (tramite legge) non richiede consenso, né si deve garantire la portabilità dei dati, ma occorre fornire l'informativa, nella quale va indicata la base giuridica del trattamento. La finalità deve essere specificata per legge.

Tipologia dati trattati: es. dati personali, dati particolari, dati biometrici, dati genetici, immagini

Descrizione dei dati trattati: Indicare ad es. per i dati personali se sono dati di contatto quali Nome cognome, indirizzi fisici e mail, contatti telefonici

In caso di trattamento di dati supersensibili presenza della garanzia anonimato per legge di settore che tecnicamente viene realizzato con l'oscuramento ossia i dati restano nella sola disponibilità dei medici/reparto/servizio curante in luogo della gestione in forma anonima?
Si ricorda che un **dato anonimo** è diverso da un dato pseudoanonimizzato.

Si ha infatti **pseudonimizzazione** quando il trattamento dei dati personali è fatto in modi tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Il dato è invece anonimo quando l'informazione è originariamente non associabile ad uno specifico interessato e neppure attraverso una successiva operazione di collegamento ad informazioni di diversa natura, risulti comunque idonea a rendere identificabile un soggetto.

Categorie dei **soggetti INTERESSATI**: L'interessato (*data subject*) al trattamento è la **persona fisica** a cui si riferiscono i dati personali. Tra gli interessati possono comparire anche minori e soggetti vulnerabili, il che comporta che il trattamento in parola, anche per tale aspetto, è soggetto a rischi per i diritti e le libertà delle persone fisiche.

Trattamento su larga scala:tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

- la durata, ovvero la persistenza, dell'attività di trattamento;

- la portata geografica dell'attività di trattamento.

es. trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;

Origine del dato: dove prendo il dato che tratto? Dall'interessato, da un soggetto terzo? E da chi?

Responsabile-i esterno-i? In quest'ambito si deve precisare anche se c'è/ci sono dei responsabili esterni designati da ASL 3 ex art. 28 Regolamento UE 2016/679 (tramite il dirigente autorizzato con compiti specifici della struttura area che effettua il trattamento) e quali sono, indicare l'avvenuta designazione, etc..

Categorie dei soggetti DESTINATARI: **Destinatari** sono, quindi, tutti i soggetti che ricevono **dati** personali dal titolare, siano essi interni od esterni. I **destinatari** possono ricevere tali **dati** per eseguire trattamenti per conto del titolare, o per conseguire proprie specifiche finalità. Specificare chi sono nel trattamento di cui trattasi.

I dati vengono trasferiti all'estero?

Precisare se intra UE od extra UE.

Si ricorda che il trasferimento può essere anche collegato all'effettuazione di un trattamento da parte di un responsabile esterno che ad es. ha un cloud all'estero.

Il trasferimento di dati personali da paesi appartenenti all´UE verso Paesi "terzi" (non appartenenti all´UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è vietato, in linea di principio, a meno che il Paese in questione garantisca un livello di protezione "adeguato" paragonabile a quello garantito dalla UE e l'interessato ne sia

Se trasferiti descrivere la base di tutela per trasferimento all'estero e se l'interessato ne è preventivamente informato

Tempi di conservazione

Indicando modalità e tempi di conservazione dei dati (con ciò facendo riferimento anche ad es.alla separazione dei dati ed alla loro criptatura; organizzazione o meno per moduli).

Criterio di calcolo dei tempi di conservazione (in alternativa) es.durata della vita dell'interessato

Specificare la **ragione della tenuta**: precisare perché devo conservare il dato

Come avviene la cancellazione : chi se ne occupa e criteri di controllo. Parimenti precisare chi si occupa e chi controlla che vengano garantiti gli altri diritti dell'interessato sui dati anche prima della scadenza dei termini di conservazione e come lo si può documentare.

Fornita **idonea informativa ai soggetti interessati.**

Consenso o elementi di esclusione del consenso (motivazione)

Modalità di acquisizione del consenso, se dovuto, ed eventuale processo di controllo

I dati vengono diffusi?

Per **diffusione** si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, ad es. diffusione anche quando si pubblica online, ad esempio una fotografia od un documento contenente dati personali.

Se diffusi specificare motivo : Precisare la base giuridica della diffusione es. pubblicità legale, normativa sulla trasparenza

Esistenza o meno di un Privacy Impact assessment **(DPIA):**
La valutazione di impatto del trattamento(D.P.I.A., cioè Data Protection Impact Assessment) è un onere posto direttamente a carico del titolare del trattamento (art. 35 GDPR) e per esso del dirigente con compiti specifici del sistema privacy aziendale che ha in carico il trattamento, col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali. E' lo strumento cardine tramite il quale il titolare effettua l'analisi dei rischi derivanti dai trattamenti posti in essere. Il titolare, quindi,deve sviluppare una valutazione preventiva (quindi prima di iniziare il trattamento) delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati. Il responsabile del trattamento, se esistente, deve
La valutazione del rischio, da realizzare per ogni singolo trattamento, dovrà portare il titolare a decidere in autonomia se sussistono **rischi elevati** inerenti il trattamento, in assenza dei quali potrà procedere oltre. Se invece ritenesse sussistenti rischi per le libertà e i diritti degli interessati, dovrà individuare le **misure specifiche richieste per attenuare o eliminare tali rischi**. Solo nel caso in cui il titolare non dovesse trovare misure idonee a eliminare o ridurre il rischio, occorrerà consultare l'Autorità di controllo. L'Autorità interviene solo *ex post* , sulle valutazioni del titolare, indicando le misure ulteriori eventualmente da implementare, fino ad eventualmente ammonire il titolare o vietare il trattamento. In ogni caso il titolare e per esso il dirigente con compiti specifici del sistema privacy aziendale che ha in carico il trattamento, dovrà giustificare le sue valutazione e rendicontarle nel registro dei trattamenti.

Rischio integrità del dato: indicare la valutazione del rischio effettuata

Rischio riservatezza del dato: indicare la valutazione del rischio effettuata

rischio disponibilità del dato: indicare la valutazione del rischio effettuata

Esistenza delle garanzie a tutela dell'esercizio dei diritti dell' interessato: trattasi dei diritti di cui agli artt. da 15 a 22 del Regolamento UE 679/2016 e norme di armonizzazione, che riconoscono, tra gli altri, il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne la rettifica ovvero l'integrazione, la cancellazione ("diritto all'oblio"), salvo i casi previsti all'art. 17 comma 3 del Regolamento UE 679/2016 e norme di armonizzazione ("**Diritto alla cancellazione («diritto all'oblio»)-** 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.") , la limitazione del trattamento, se ricorrano le ipotesi di cui all'art. 18 del Regolamento UE 679/2016 e norme di armonizzazione **("Diritto di limitazione di trattamento").** l'opposizione al loro trattamento ai sensi dell'art. 21 del regolamento UE 679/2016 e norme di armonizzazione **("Diritto**
Nonché il diritto di proporre reclamo all'Autorità di controllo (Autorità Garante per la protezione dei dati personali- secondo le modalità previste sul sito internet dello stesso **www.garanteprivacy.it**) nei casi previsti dalle disposizioni in materia di protezione dei dati di cui al Regolamento UE 679/2016 e norme di armonizzazione. Indicare le modalità attraverso le quali all'interessato viene garantito l'esercizio dei diritti che gli sono riconosciuti ex artt.15-23 Regolamento UE 206/679 e se ne è stata data allo stesso specifica informazione e con che modalità. Si ricorda che a seconda del trattamento potrebbe essere necessario precisare la non esercitabilità di alcuni diritti e le relative motivazioni (es.divieto

ffettuata.