**Valutazione d'impatto sulla protezione dei dati personali ai sensi dell'Art.35 del Regolamento UE n.679/2016 relativo al trattamento "Progetto di ricerca retrospettivo per valutazioni su prestazioni di un saggio automatizzato"**

## 1. Descrizione del trattamento

Diasorin Italia S.p.A. ("Diasorin Italia") intende condurre uno studio osservazionale di tipo retrospettivo-prospettico ("Studio") utilizzando campioni biologici congelati, originariamente raccolti dalla Azienda USL di Modena (residui di test svolti dalla stessa USL in passato) e riferibili a testati per marcatori tiroidei.

I Dati di cui l'Azienda USL Modena dispone saranno pseudonimizzati dall'Azienda stessa e trasferiti a Diasorin Italia, affinché possa effettuare lo Studio.

Lo scopo dello studio è di valutare un saggio automatizzato verificando le prestazioni diagnostiche sulla base dell'evidenza clinica (in base alla tipologia dei pazienti analizzati) o su confronto tra metodiche.

I dati saranno trattati esclusivamente per la finalità di cui sopra. Non saranno trattati per finalità diagnostiche.

## 2. Quadro normativo

### *2.1. Le prescrizioni del GDPR e la necessità di effettuare una DPIA*

Pilastro del Regolamento UE n.679/2016 ("GDPR") è il principio "*accountability*", in forza del quale i titolari e i responsabili del trattamento devono adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare il rispetto e l'applicazione della normativa privacy.

Con il principio di *accountability*, il legislatore europeo ha voluto sostituire un approccio di tipo prescrittivo (unico per tutti, *one size fits all*) con un approccio basato sul rischio (*risk based*).

Strettamente connessi al principio di accountability sono i principi di "*data protection by design and by default*" (art. 25 GDPR), che impongono al Titolare ed al Responsabile del trattamento di valutare, sin dalla progettazione delle modalità di trattamento dei dati (*by design*), la natura delle attività di trattamento che si intende porre in essere ed i rischi che tali attività possono comportare, apportando, per impostazione predefinita (*by default*), tutte le misure necessarie a garantire un' effettiva e adeguata protezione dei dati personali degli interessati.

Dunque, alla luce di tale assetto normativo, il Titolare ed il Responsabile del trattamento sono tenuti a predisporre fin dall'inizio garanzie idonee a soddisfare le prescrizioni del GDPR ed atte a tutelare i diritti degli interessati.

### 2.2. La normativa (nazionale) in materia di protezione dei dati personali

Il D. Lgs. 10 agosto 2018 n. 101 ha adeguato la normativa nazionale (D. Lgs. 30 giugno 2003 n. 196 – "Codice privacy") alle disposizioni del GDPR.

L'articolo 110 del Codice Privacy, relativamente al trattamento di dati personali per le finalità di ricerca medica, biomedica ed epidemiologica, prevede delle deroghe al principio (stabilito all'Art. 9, c.2, lett. a) per cui i dati relativi alla salute possano essere trattati esclusivamente previo consenso dell'interessato.

Condizione necessaria affinché possano trovare applicazione tali deroghe è la predisposizione e pubblicazione di una valutazione d'impatto ai sensi degli Artt. 35 e 36 del GDPR.

La presente valutazione d'impatto viene quindi redatta in ottemperanza a quanto previsto dalla summenzionata normativa.

## 3. Modalità di trattamento

### 3.1. Ruoli privacy

L'Azienda USL di Modena e Diasorin Italia si qualificheranno come autonomi Titolari del Trattamento.

### 3.2. Categorie di soggetti interessati

Diasorin Italia tratterà – in forma completamente pseudonimizzata – i dati delle seguenti categorie di soggetti interessati:

- Pazienti
- Pazienti minorenni

### 3.3. Categorie di Dati Personali oggetto del Trattamento

Diasorin Italia riceverà le seguenti categorie di dati personali (pseudonimizzati) riferibili ai pazienti (sia maggiorenni che minorenni):

- data di raccolta del campione;
- età del paziente;
- sesso del paziente;
- motivazioni per cui è stato svolto il test;
- Risultati di test di laboratorio relativi a marcatori tiroidei;
- informazioni relative alla terapia somministrata;
- eventuale presenza di patologie autoimmuni;
- eventuale presenza di patologie tiroidee;
- eventuale stato di gravidanza della paziente.

Qualora il paziente fosse regolarmente monitorato presso il centro sarà effettuata un'attività di *follow-up* su un paziente, il quale sarà identificato tramite il codice alfanumerico fornito

originariamente dalla Azienda USL di Modena, per permettere la valutazione di campioni sequenziali già disponibili presso il centro  Non saranno in alcun caso trattati dati ulteriori rispetto a quelli sopra elencati e il paziente, anche a seguito di questo ulteriore trattamento, non rimarrà in alcun modo identificabile da parte di Diasorin Italia.

### 3.4. Modalità di raccolta del Dato

I Dati Personali riferibili al singolo paziente sono stati originariamente raccolti dalla Azienda USL di Modena per svolgere tutte le necessarie attività di analisi e di cura.

Su richiesta di Diasorin Italia, Azienda USL di Modena tratterà i dati di cui dispone al fine di pseudonimizzarli e di assegnare ad ogni paziente un codice alfanumerico ("ID"). I dati così pseudonimizzati saranno raccolti in un file Excel protetto da password, che verrà inviato a Diasorin Italia.

Diasorin Italia potrà conoscere, dunque, solo l'ID affidato al paziente. Non potrà accedere, per nessuna circostanza, alla "chiave di lettura" per decifrare i dati. Diasorin Italia non potrà in alcun modo risalire all'identità del paziente.

### 3.5. Base giuridica del Trattamento

Diasorin Italia considera applicabile al trattamento di cui alla presente DPIA la deroga, di cui all'Art.110 Codice Privacy, al divieto di trattare i dati relativi alla salute senza aver ottenuto il consenso dell'interessato (Art.9, c.2, lett. a) GDPR). Dal momento che Diasorin Italia riceve solo dati pseudonimizzati, sarebbe impossibile ottenere il consenso del soggetto interessato al trattamento, dal momento che non è identificabile.

Allo stesso modo, i dati non saranno ricevuti sulla base di un consenso al ri-utilizzo del dato da parte di un terzo, ottenuto dalla Azienda USL di Modena, in quanto rappresenterebbe per il Titolare originario del dato un onere sproporzionato ricontattare i pazienti relativamente ad un campione biologico già ottenuto.

### 3.6. Condivisione dei Dati

Diasorin Italia tratterà i dati solo internamente. Questi non saranno condivisi con soggetti terzi.

I Dati saranno trattati esclusivamente dal personale di Diasorin Italia adeguatamente istruito e nominato Autorizzato al Trattamento, ai sensi dell'Articolo 29 GDPR.

## 4. Valutazione di necessità e proporzionalità del trattamento

| | |
|---|---|
| Le finalità sono specifiche, esplicite e legittime? | Sì, il trattamento sarà svolto in conformità a quanto previsto dall'Art. 110 Codice Privacy. |
| Il trattamento è svolto in modo lecito? | Sì, il trattamento sarà svolto in conformità a quanto previsto dall'Art. 110 Codice Privacy. |

| | |
|---|---|
| I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario? | Sì, verranno raccolti solo i dati strettamente necessari alla realizzazione dello Studio. Inoltre, i dati saranno opportunamente pseudonimizzati da parte della Azienda USL di Modena. Diasorin Italia li riceverà senza "chiave di lettura", in modo che non possa in alcun modo risalire all'identità dell'interessato. Le analisi effettuate sui campioni ricevuti verranno completate preferibilmente entro 4 settimane dal momento in cui questi vengono ricevuti da Diasorin Italia. I dati verranno conservati dal centro per 7 anni, coerentemente con il contratto di studio delle prestazioni in essere con lo stesso. Diasorin Italia conserverà i dati in conformità alle previsioni di cui al regolamento UE 2017/746 relativo ai dispositivi medico-diagnostici in vitro. Al momento della cancellazione dei dati da parte del centro - poiché verrà eliminata altresì l'esistente "chiave di lettura" del dato pseudonimizzato - le informazioni ricevute da DiaSorin Italia saranno totalmente anonimizzate e non si qualificheranno più come dati personali. |

### 4.1. Definizione delle misure idonee ad escludere o mitigare il rischio

| Misure/ Controlli specifici | Implementazione | Note (eventuali) |
|---|---|---|
| Finalità: specifiche, legittime ed esplicite | SÌ | In ottemperanza a quanto previsto dall'Art.110 Codice Privacy, le finalità e le garanzie del trattamento vengono esposte nella presente DPIA, che sarà resa pubblica affinché il pubblico possa conoscere in maniera puntuale i trattamenti effettuati. |
| Liceità del trattamento | SÌ | In ottemperanza a quanto previsto dall'Art.110 Codice Privacy, dal momento che per Diasorin Italia non sarebbe possibile richiedere il consenso degli interessati, le finalità e le garanzie del trattamento vengono esposte nella presente DPIA, che sarà resa pubblica affinché il pubblico possa conoscere in maniera puntuale i trattamenti effettuati. |
| Minimizzazione: informazioni adeguate, rilevanti e limitate | SÌ | Saranno raccolti esclusivamente i dati strettamente necessari alla realizzazione delle Studio. Le categorie di dati necessari sono state oggetto di valutazione da parte dei |

| | | |
|---|---|---|
| | | progettatori dello studio e comunicate alla Azienda USL di Modena. L'Azienda non invierà alcun dato ulteriore rispetto a quelli richiesti da Diasorin Italia.<br>I dati saranno opportunamente pseudonimizzati dalla Azienda USL di Modena ed inviati a Diasorin Italia senza "chiave di lettura".<br>I dati saranno conservati dal centro per un massimo di 7 anni. Successivamente alla cancellazione da parte del centro, Diasorin Italia conserverà le informazioni in forma totalmente anonimizzata (dunque, non si qualificheranno più come dati personali). |
| Qualità dei dati: accurati e aggiornati | SÌ | Dal momento che Diasorin Italia tratterà campioni biologici, il dato farà riferimento al momento in cui il campione è stato raccolto.<br>Diasorin Italia valuterà, , l'utilizzo di campioni e dati di follow-up su i pazienti già regolarmente monitorati ed identificati tramite codice alfanumerico. |
| Conservazione | SÌ | Diasorin Italia tratterà i dati per tutta la durata dello studio. I dati saranno conservati presso Diasorin Italia coerentemente con la normativa vigente.<br>In particolare, i dati saranno conservati dal centro per un massimo di 7 anni. Successivamente alla cancellazione da parte del centro, Diasorin Italia conserverà le informazioni in forma totalmente anonimizzata |

### 4.2. Misure adottate per garantire l'esercizio dei diritti degli interessati

| **Misure/ Controlli specifici** | **Implementazione** | **Note (eventuali)** |
|---|---|---|
| Informativa: chiara e facilmente accessibile | | Diasorin Italia riceverà solamente dati pseudonimizzati senza "chiave |

| Misure/ Controlli specifici | Implementazione | Note (eventuali) |
|---|---|---|
| redatta ai sensi degli artt. 13 e 14 del GDPR | | di lettura". Non essendo in grado di risalire all'identità degli interessati, Diasorin Italia non fornirà l'informativa. Ai sensi di quanto previsto dall'Art.110 Codice Privacy, dal momento che non sarebbe possibile raccogliere il consenso degli interessati, sarà resa pubblica la presente DPIA al fine di descrivere i trattamenti effettuati. |
| Diritto di accesso | SÌ | In qualunque momento, un soggetto interessato potrà contattare il Titolare all'indirizzo PEC diasorinitalia@pecdotcom.it ed ottenere conferma che sia o meno in corso un Trattamento dei Suoi Dati Personali, e, nel caso, richiedere l'accesso ai Dati, ai sensi dell'Art.15 GDPR. |
| Diritto di portabilità | | Il trattamento dei dati non viene effettuato sulla base del consenso dell'interessato o della necessità di dare esecuzione al contratto. In ogni caso, qualora l'interessato lo richieda, laddove tecnicamente fattibile, Diasorin Italia comunicherà i dati direttamente all'interessato o ad altro Titolare, ai sensi dell'Art.20 GDPR. |
| Diritto di revoca del consenso precedentemente espresso | | Il trattamento dei dati non viene effettuato sulla base del consenso dell'interessato. |
| Diritto di rettifica | SÌ | In qualunque momento, un soggetto interessato potrà contattare il Titolare all'indirizzo PEC diasorinitalia@pecdotcom.it e ottenere la rettifica di dati personali inesatti. |
| Diritto di cancellazione | SÌ | In qualunque momento, un soggetto interessato potrà contattare il Titolare all'indirizzo PEC diasorinitalia@pecdotcom.it e chiedere la cancellazione di Dati Personali che non siano più necessari per le finalità perseguite, |

| Misure/ Controlli specifici | Implementazione | Note (eventuali) |
|---|---|---|
| | | di quelli per i quali ha esercitato il Diritto di opposizione o di quelli che devono essere cancellati al fine di adempiere un obbligo legale, ai sensi dell'Art.17 GDPR. |
| Diritto di limitazione | SÌ | In qualunque momento, un soggetto interessato potrà contattare il Titolare all'indirizzo PEC diasorinitalia@pecdotcom.it e ottenere dal Titolare la limitazione del Trattamento con riferimento a Dati Personali di cui sia contestata l'esattezza o di cui Diasorin Italia non abbia più bisogno ai fini del trattamento, ai sensi dell'Art.18 GDPR. |
| Diritto di opposizione | SÌ | In qualunque momento, un soggetto interessato potrà contattare il Titolare all'indirizzo PEC diasorinitalia@pecdotcom.it e opporsi al trattamento dei propri dati personali, ai sensi dell'Art.21 GDPR. |

## 5. Analisi del rischio e misure di sicurezza

### 5.1. Il rapporto tra le tipologie di trattamento e le finalità (necessità e proporzionalità del trattamento)

Il trattamento dei dati avverrà nel rispetto dei principi generali prescritti dal GDPR. In particolare, è necessario che il trattamento rispetti i principi di proporzionalità e minimizzazione: il Titolare è tenuto a dimostrare di aver richiesto le sole informazioni necessarie per il perseguimento delle specifiche finalità, al fine di evitare che i dati oggetto di trattamento possano essere considerati eccedenti.

Il rapporto tra necessità e proporzionalità dei trattamenti effettuati nell'ambito del Progetto, viene altresì garantito dalle misure di sicurezza che verranno implementate e che sono compiutamente descritte nei paragrafi che seguono.

### 5.2. I rischi possibili connessi al trattamento – considerazioni generali

Le violazioni del GDPR possono causare danni "materiali" o "immateriali". Tra questi ultimi possono rientrare: la perdita del controllo sui dati personali, la limitazione dei diritti, la perdita di riservatezza; tra quelli materiali, invece, rientrano non solo le violazioni delle misure di sicurezza ma anche le perdite finanziarie e gli altri rischi economici.

Con riferimento al trattamento in esame, sono state individuate 3 tipologie di rischio a cui i dati personali potrebbero potenzialmente essere esposti, in particolare

(i) rischi interni (ossia arrecati da dipendenti, collaboratori del Titolare);
(ii) rischi esterni (ossia imputabili, ad esempio, al trattamento da parte di soggetti terzi);
(iii) rischi imputabili ad agenti esterni quali, per esempio: incidenti informatici; disastri naturali.

Come noto, il GDPR individua specifiche misure di sicurezza da adottare per garantire la tutela dei diritti e le libertà dei soggetti interessati. In particolare:

(i) la pseudonimizzazione e la cifratura dei dati personali;
(ii) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
(iii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
(iv) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Diasorin Italia riceverà dalla Azienda USL di Modena e tratterà i dati esclusivamente in forma pseudonimizzata. Gli accordi conclusi con la Azienda USL di Modena prevedono che in alcun caso sarà inviata a Diasorin Italia la chiave per decifrare i Dati Personali.

In tal modo, Diasorin Italia garantisce l'assoluta riservatezza dei dati dei pazienti.

I dati pseudonimizzati saranno trasferiti tramite file Excel protetto da username e password

Inoltre, i trattamenti che Diasorin Italia ha intenzione di effettuare non rientrano tra quelli elencati all'Art.35 GDPR, i quali potrebbero presentare rischi elevati per i diritti e le libertà delle persone fisiche. In particolare:

- non verranno effettuati trattamenti integralmente automatizzati.

- i dati saranno trattati solo per il fine di migliorare gli strumenti diagnostici prodotti da Diasorin Italia. Diasorin Italia non assumerà decisioni che potrebbero avere effetti giuridici o che incidano in modo analogo sulle persone fisiche.

- i soggetti interessati dal trattamento sono solamente i pazienti della Azienda che hanno eseguito test per marcatori tiroidei. Dunque, il trattamento non sarà effettuato su larga scala.

- non sarà impiegato l'uso di nuove tecnologie

**5.1. *È prevista altresì l'adozione delle seguenti misure tecniche di sicurezza***

- i dati verranno conservati su infrastruttura IT di proprietà e gestita da Diasorin Italia

- l’infrastruttura IT è costantemente monitorata per ridurre al minimo gli incidenti di sicurezza informatica
- l’accesso ai dati sarà controllato tramite gestione degli accessi con definizione degli appropriati permessi
- i dati saranno soggetti alle esistenti politiche di backup di Diasorin Italia
- l’efficacia delle misure verrà verificata su base annuale come da politiche di gestione interne a Diasorin Italia

## 6. Livello di rischio per l’interessato

Alla luce di quanto esposto, si ritiene che il livello di rischio per i diritti e le libertà dei soggetti Interessati sia basso.

Ai sensi di quanto previsto dall’Art.36 GDPR, si ritiene non necessario consultare l’Autorità Garante per la Protezione dei Dati Personali (“Garante”) e si decide di procedere in tal senso.

## 7. Parere del DPO

Il DPO valuta positivamente conclusa la presente DPIA relativa al descritto Progetto di ricerca retrospettivo.

IL DPO, considerate le misure determinate per garantire l’impossibilità di ricondurre il dato ad una persona fisica e le garanzie adottate per tutelare i diritti e le libertà degli interessati, concorda nel ritenere che il trattamento presenti un livello di rischio basso.

Si raccomanda alla Società di monitorare qualsiasi mutamento nel previsto trattamento dei dati e di descriverlo all’interno della presenta DPIA. A tal proposito, andranno previste verifiche periodiche volte ad accertare che l’architettura del progetto non presenti delle modifiche che richiedano un’ulteriore valutazione.

Qualora si verificassero mutamenti che comportino un innalzamento del livello di rischio, si raccomanda di procedere con la Consultazione Preventiva al Garante, ai sensi di quanto previsto dall’Art.36 GDPR.

Con l’entrata in vigore del DDL n.1110 di conversione in legge del Decreto Legge 2 marzo 2024, n.19, il giorno 23 aprile 2024, è stata approvata la riforma dell’Art.110 Codice Privacy, laddove prevedeva l’obbligo di Consultazione Preventiva al Garante (ai sensi dell’Art.36 GDPR), per i trattamenti di dati personali per ricerca medica, biomedica ed epidemiologica, nei casi in cui non fosse necessario il consenso dell’interessato.

Tale previsione è stata sostituita dall’obbligo di osservare le garanzie individuate dal Garante ai sensi dell'articolo 106, comma 2, lettera d), del Codice Privacy. Ai sensi dell’Art. 106 Codice Privacy, il Garante promuove regole deontologiche, per i soggetti pubblici e privati, inerenti al

trattamento dei dati per fini statistici o di ricerca scientifica, volte ad individuare garanzie adeguate per i diritti e le libertà dell'interessato, in conformità dell'Art.89 GDPR.

Con tali regole deontologiche, sono individuate le garanzie da osservare "*nei casi in cui si può prescindere dal consenso dell'interessato*" (Art.106, comma 2, lett.b) Codice Privacy).

Alla luce di ciò, il DPO raccomanda di monitorare le attività del Garante volte all'adozione di regole deontologiche applicabili al progetto di ricerca retrospettivo. Qualora future regole deontologiche comportassero la necessità di modificare alcuni aspetti del trattamento posto in essere, il Titolare dovrà immediatamente adeguarsi a tali previsioni e aggiornare la presente DPIA.

Saluggia, 29 aprile 2024

Il DPO

Avv. Ulisse Spada