Allegato 1

Direzione Regionale Lombardia

A Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico
protocollo@pec.policlinico.mi.it

Oggetto: Allegato Privacy alla "Convenzione per l'effettuazione di controlli ergoftalmologici ed eventuali visite oculistiche di completamento per i dipendenti Inail della Direzione regionale e per le sedi di Milano nord-est, Milano centro-Legnano, Milano sud-Lodi e Sesto San Giovanni e Rho".

PREMESSA

Il presente documento ("Allegato") è redatto in conformità a quanto previsto all'art. 28 del Regolamento (UE) 2016/679 e forma parte integrante e sostanziale della Convenzione stipulata tra le Parti, come definito all'articolo 7 della suddetta Convenzione.

Il fornitore, come sotto definito, ha dichiarato, di essere in grado di assicurare idonee e adeguate garanzie in termini di conoscenza specialistica, affidabilità, risorse, nonché in ordine all'adozione di misure tecniche, logiche ed organizzative per assicurare che i trattamenti dei dati personali siano conformi alle esigenze del Regolamento Europeo. Con la sottoscrizione della Convenzione e del presente Allegato, che ne costituisce parte integrante, il Responsabile dichiara altresì di essere consapevole, di essere nominato con la sottoscrizione del presente Allegato Responsabile del trattamento in funzione della designazione fatta da Inail in qualità di Titolare, nel presente Allegato.
Il Titolare e il Responsabile sono di seguito nominati disgiuntamente la Parte e congiuntamente le "Parti".

Il mancato rispetto delle disposizioni di cui al presente Allegato sarà considerato un grave inadempimento della Convenzione stessa.

Ai fini del presente Allegato con il termine "Fornitore" o "Responsabile del trattamento" si individua l'Impresa appaltatrice designata quale Responsabile del trattamento ai sensi del Regolamento (UE) 2016/679 o GDPR in ragione delle prestazioni oggetto della Convenzione.

Pertanto, ai fini del presente Allegato e delle sue successive modifiche/integrazioni concordate in forma scritta tra le Parti, le Parti espressamente convengono che:

- La Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico Responsabile è di seguito definita come Responsabile o Responsabile del trattamento dei Dati Personali
- Inail è definito come Titolare del trattamento dei Dati Personali.

OGGETTO E DURATA DEL PRESENTE ALLEGATO

1. Il presente Allegato disciplina le istruzioni che il Responsabile si impegna ad osservare nell'ambito dei trattamenti dei Dati Personali che realizzerà per conto del Titolare nello svolgimento delle attività oggetto della Convenzione in vigore garantendo la conformità alla normativa vigente in materia di tutela e sicurezza dei Dati Personali.
2. La durata di efficacia del presente Allegato, che è parte della Convenzione a cui si riferisce, decorre dalla sua sottoscrizione ovvero alla data di cessazione della Convenzione.
3. Le Parti espressamente convengono che in caso di contrasto tra le disposizioni contenute nel presente Allegato e le Norme in materia di Trattamento dei Dati Personali come sotto definite e le loro successive modifiche/integrazioni, queste ultime si riterranno prevalenti.
4. In caso di contrasto tra le disposizioni contenute nel presente Allegato e qualsiasi disposizione contenuta nella Convenzione con riferimento alla Privacy, le norme contenute nel presente Allegato si riterranno prevalenti.

DEFINIZIONI

- "Dati Personali": i Dati Personali di cui all'art. 4 del Regolamento UE 2016/279 (nonché i dati appartenenti alle categorie particolari di dati personali di cui all'art. 9 e 10 del Regolamento UE 2016/679).
- "Tipo di Dati Personali trattati": dati anagrafici e sanitari;
- "Categorie di soggetti interessati": dipendenti INAIL;
- "Norme in materia di Trattamento dei Dati Personali": tutte le leggi, disposizioni e direttive normative applicabili in relazione al trattamento e/o alla protezione dei Dati Personali, così come modificate di volta in volta, ivi incluso, ma non limitatamente, il Regolamento UE 2016/679 (GDPR), la normativa di adeguamento italiana, circolari, pareri e direttive dell'Autorità di Controllo nazionale, le decisioni interpretative adottate dall'European Data Protection Board (EDPB).

- "Convenzione": si intende la Convenzione stipulata tra il Titolare e il Responsabile avente ad oggetto l'effettuazione di controlli ergoftalmologici ed eventuali visite oculistiche di completamento per i dipendenti Inail della Direzione regionale e per le sedi di Milano nord-est, Milano centro-Legnano, Milano sud-Lodi e Sesto San Giovanni e Rho.

- "Misure di Sicurezza": le misure di sicurezza di natura fisica, logica, tecnica e organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio, ivi comprese quelle specificate, nella Convenzione unitamente ai suoi Allegati.
- "Sub-Responsabile del trattamento": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che svolge l'attività di responsabile del trattamento in forza di contratto scritto con il Responsabile del trattamento; Le Parti convengono che il Responsabile del trattamento non ricorrerà a un altro Responsabile, che opererà in qualità di Sub- responsabile senza previa autorizzazione scritta, specifica o generale, da parte del Titolare del trattamento.

- "Persone autorizzate al trattamento dei dati": persone che in qualità di dipendenti, collaboratori, amministratori o consulenti del responsabile e/o del sub-responsabile siano state autorizzate al trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile.
- "Violazione dei Dati Personali (data breach)": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.
- "Incidente di sicurezza": la violazione di sicurezza che comporta la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati e/o informazioni riservate la violazione e/o il malfunzionamento di misure di sicurezza, di strumenti elettronici, hardware o software a protezione dei dati e delle informazioni.
- Per quanto non espressamente ivi richiamato nelle Definizioni di cui al presente Allegato, le Parti rinviano alle definizioni di cui all'art. 4 del Regolamento (UE) 2016/679.

SICUREZZA DEI DATI PERSONALI

Il Responsabile ottempererà a tutte le norme in materia di Trattamento dei Dati Personali in relazione al Trattamento dei Dati Personali ivi comprese quelle che saranno emanate nel corso della durata della Convenzione al fine di assicurare, ciascuno nell'ambito delle proprie attività e competenze specifiche, un adeguato livello di sicurezza dei trattamenti, inclusa la riservatezza e in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta.

OBBLIGHI E ISTRUZIONI PER IL RESPONSABILE

I. OBBLIGHI GENERALI DEL FORNITORE

1. Ai sensi del presente Allegato, il Responsabile è autorizzato a trattare per conto del Titolare i Dati Personali necessari per l'esecuzione delle attività di cui all'oggetto della Convenzione.
2. A tal fine il Responsabile si impegna a:
   - non determinare o favorire mediante azioni e/o omissioni, direttamente o indirettamente, la violazione da parte del Titolare del trattamento delle Norme in materia di Trattamento dei Dati Personali;
   - trattare i Dati Personali esclusivamente in conformità al presente Allegato, e pertanto nella misura ragionevolmente necessaria all'esecuzione della Convenzione, e in conformità alle Norme in materia di Trattamento dei Dati Personali;
   - adottare, Misure di sicurezza come di seguito previste e in ogni caso adeguate a garantire la protezione e la sicurezza dei Dati Personali al fine di prevenire a titolo indicativo e non esaustivo:
     - incidenti di sicurezza; violazioni dei Dati Personali (Data Breach)
     - ogni violazione delle misure di sicurezza;
     - tutte le altre forme di Trattamento dei dati non autorizzate o illecite.
3. Il Responsabile si impegna a designare il Responsabile della protezione dei dati di cui all'art. 37 GDPR e a comunicarne i dati e i contatti di riferimento tempestivamente al Titolare in ragione dell'attività svolta.
4. [CASO AUTORIZZAZIONE GENERALE: il Responsabile del trattamento comunica in forma scritta al Titolare del trattamento entro un mese precedenti alla relativa modifica - eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche];

II. ISTRUZIONI PER IL FORNITORE

II.A) Elementi essenziali delle istruzioni

Gli elementi essenziali del trattamento sono contenuti nel presente Allegato.

II.B) Obblighi del Responsabile nei confronti del Titolare

Il Responsabile si impegna a:

1. Trattare i dati solo per l'esecuzione delle attività di cui all'oggetto della Convenzione;
2. Trattare i dati conformemente alle istruzioni documentate impartite dal Titolare del trattamento (con il presente Allegato e con eventuali ulteriori integrazioni al presente Allegato, in ogni caso sottoscritte da entrambe le Parti);
3. Qualora il Responsabile reputi che un'istruzione sia, o possa essere, contraria alla Normativa in materia di protezione dei dati, ivi incluso il GDPR, deve informarne immediatamente e in forma scritta il Titolare del Trattamento;
4. Garantire che il trattamento dei Dati Personali sia effettuato in modo lecito, corretto, adeguato, pertinente e avvenga nel rispetto dei principi di cui all'artt. 5 e ss. del GDPR;
5. Garantire la riservatezza dei Dati Personali trattati per l'esecuzione delle attività della Convenzione;
6. Garantire che le Persone autorizzate a trattare i Dati Personali in virtù della presente Convenzione: *i)* si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; *ii)* abbiano ricevuto, e ricevano, da parte del Responsabile la formazione necessaria in materia di protezione dei Dati Personali; *iii)* accedano e trattino i Dati Personali osservando le istruzioni impartite dal Titolare del trattamento, in ogni caso conformemente alle disposizioni di cui al presente Allegato;
7. Tenere conto nell'esecuzione delle attività di cui alla Convenzione dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (privacy by design e by default);

8. Qualora richiesto dalle Norme in materia di Trattamento dei Dati Personali, il Titolare e il Responsabile convengono di sottoscrivere un accordo aggiuntivo, di modifica o di aggiornamento che potrà essere necessario in ogni caso conforme alle Norme sul Trattamento dei Dati Personali;

II.C) Obblighi del Responsabile nell'ambito dei diritti esercitati dagli Interessati nei confronti del Titolare

1. Il Responsabile collabora nella misura in cui questo sia possibile e per quanto di sua competenza alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-22 del GDPR;
2. Il Fornitore, tenuto conto della natura del trattamento, assiste il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui questo sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
3. il Responsabile adotta e aggiorna un registro di tutte le attività di trattamento eseguite per conto del Titolare e completo di tutte le informazioni previste all'art. 30 del GDPR;
4. Qualora il Responsabile riceva una comunicazione inerente all'esercizio dei diritti dell'interessato, che dovrebbe essere in ogni caso rivolta al Titolare, il Fornitore, si impegna ad inoltrarla tempestivamente, e comunque entro e non oltre 7 giorni dalla ricezione, per posta elettronica al Titolare del trattamento.

II.D) Obblighi del Responsabile che ricorre a Persone Autorizzate al trattamento dei Dati Personali

1. Ai sensi dell'art. 28 GDPR, paragrafo 3, b) il Responsabile si obbliga ai sensi del presente Allegato a garantire che le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Responsabile

ovvero Responsabile del trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

III. IL REGISTRO DEI TRATTAMENTI DEL RESPONSABILE

1. Il Responsabile predispone, un registro, in formato elettronico di tutte le categorie di attività relative ai trattamenti svolti per conto del Titolare del Trattamento, come prevede l'art. 30, paragrafo 2, del GDPR.
2. In particolare, il Registro dei trattamenti del Responsabile relativo ai trattamenti eseguiti per conto del Titolare deve contenere:
   a) il nome e i dati di contatto del Responsabile in qualità di Responsabile del trattamento, di ogni Titolare del trattamento per conto del quale il Responsabile agisce, del rappresentante (eventuale) del Responsabile o del Titolare del trattamento nonché del Responsabile della protezione dei dati (DPO);
   b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
   c) una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto per un trattamento corretto e sicuro sensi dell'articolo 32 del GDPR.

IV. COLLABORAZIONE DEL RESPONSABILE NELL'ADEMPIMENTO DEGLI OBBLIGHI DEL TITOLARE

Il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento.

~~a)~~

V. ULTERIORI OBBLIGHI DI GARANZIA DEL RESPONSABILE

Il Responsabile si impegna a:

1. mettere a disposizione del Titolare del trattamento tutte le informazioni essenziali a dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

   Inoltre, il Responsabile del trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei Dati Personali.
2. Trattare i Dati Personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento dei Dati Personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o Nazionale cui è soggetto il Responsabile del trattamento. In Tale caso il Responsabile del trattamento informa il Titolare di tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.
3. Il Responsabile si impegna a notificare tempestivamente al Titolare ogni provvedimento di un'Autorità di controllo, o dell'Autorità giudiziaria relativo ai Dati Personali del Titolare salvo il caso in cui tale comunicazione sia vietata dal provvedimento o dalla legge. In simili circostanze, e in ogni caso conformemente a quanto previsto dal GDPR e dalla normativa applicabile, il Responsabile deve: i) informare il Titolare tempestivamente e in ogni caso entro trenta giorni dalla conoscenza del provvedimento; ii) collaborare con il Titolare, iii) garantire il trattamento riservato di tali informazioni.
4. Il Responsabile si impegna a tenere indenne il Titolare per qualsiasi responsabilità connessa ad eventuali inadempimenti della normativa GDPR e relativa alla sicurezza informatica da parte del Fornitore.

5. Il Titolare si impegna a tenere indenne il Responsabile per qualsiasi responsabilità connessa ad eventuali inadempimenti della normativa GDPR e relativa alla sicurezza informatica da parte del Titolare del trattamento.

VI. OBBLIGHI DEL RESPONSABILE AL TERMINE DELLA CONVENZIONE.

1. Il Responsabile si impegna a non conservare - nonché a garantire che le Persone Autorizzate al trattamento non conservino - i Dati Personali per un periodo di tempo ulteriore al limite di durata strettamente necessario per l'esecuzione dei servizi e/o l'adempimento degli obblighi di cui alla Convenzione, comunque non superiore a 3 mesi, e in ogni caso così come disciplinato dalla legge applicabili in materia.
2. Al termine della Convenzione il Responsabile si impegna a restituire al Titolare tutti i Dati Personali e a cancellare tutte le relative copie esistenti, fatto salvo quanto diversamente disposto dalle Norme in materia di Trattamento dei Dati Personali.
3. Il Responsabile deve documentare per iscritto al Titolare sia la restituzione che la cancellazione.

VII. MODIFICHE DELLE LEGGI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

In caso di modifica delle Norme in materia di Trattamento dei Dati Personali applicabili al trattamento dei Dati Personali, il Responsabile e il Titolare collaboreranno, per quanto di propria competenza, affinché siano sviluppate, adottate e implementate misure di adeguamento al GDPR e alle sue successive modifiche e integrazioni durante il periodo di efficacia della Convenzione.

VIII. DISPOSIZIONI FINALI

1. Le Parti convengono che le disposizioni di cui al presente Allegato costituiscono l'intera contrattazione tra le Parti in relazione al suo oggetto.
2. Le Parti convengono che qualsiasi modifica al presente Allegato sarà efficace e vincolante tra le Parti solo se definita di comune accordo tra le Parti e in forma scritta.
3. Nessuna delle Parti assumerà obbligazioni per conto dell'altra. Le Parti convengono di essere soggetti giuridici indipendenti.
4. La nullità di una singola clausola non comporta la nullità dell'intero Allegato.
5. Le Parti si danno reciprocamente atto che le disposizioni di cui al presente Allegato, costituiscono la sostanziale volontà tra le Parti, e che l'Allegato stato in ogni caso oggetto di trattative tra le Parti.

Per conto del titolare
Il Direttore della Direzione regionale Lombardia
dott.ssa Alessandra Lanza

Per accettazione del responsabile del trattamento
dott. Matteo Stocco