

ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI

Il presente Accordo sul trattamento dei dati personali ("DPA") (basato su Clausole Contrattuali Tipo della Commissione Europea tra titolari e responsabili del trattamento ex art. 28(7) del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, "RGPD") è incorporato nelle **"Condizioni Generali per l'Attivazione dell'account Develop-Players, la Registrazione al sito e la Fruizione delle funzionalità e/o servizi attivabili sui canali digitali di Develop-Players"** (di seguito anche solo "Contratto" o "Contratto principale") sottoscritte tra le parti, e riguarda il trattamento dei dati personali effettuato da Develop-Players S.r.l. per conto del Cliente.

Se non diversamente definito nel presente DPA, tutti i termini in maiuscolo utilizzati nel presente DPA avranno il significato loro attribuito nel Contratto.

SEZIONE I

Clausola 1 - Scopo e ambito di applicazione

- (a) Scopo delle presenti clausole contrattuali tipo (di seguito "clausole") è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("RGPD").
- (b) I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del RGPD.
- (c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.
- (d) Gli allegati da I a IV costituiscono parte integrante delle clausole.
- (e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del RGPD.
- (f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del RGPD.

Clausola 2 - Invariabilità delle clausole

- (a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.
- (b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3 - Interpretazione

- (a) Quando le presenti clausole utilizzano i termini definiti nel RGPD, tali termini hanno lo stesso significato di cui al regolamento interessato.
- (b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del RGPD.
- (c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal RGPD o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4 - Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 - Clausola di adesione successiva

- (a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.
- (b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.
- (c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II

-

OBBLIGHI DELLE PARTI

Clausola 6 - Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7 - Obblighi delle parti

7.1. Istruzioni

- (a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.
- (b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il RGPD o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

- (a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.
- (b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati ("dati sensibili"), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto

- (a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.
- (b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.
- (c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal RGPD. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

- (d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.
- (e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

- (a) **AUTORIZZAZIONE SCRITTA GENERALE** Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 30 giorni, dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.
- (b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del RGPD.
- (c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.
- (d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.
- (e) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

- (a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del RGPD.
- (b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del RGPD, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del RGPD utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del RGPD, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8 - Assistenza al titolare del trattamento

- (a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.
- (b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempire agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.
- (c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, paragrafo 2, il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:
 - (i) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali ("valutazione d'impatto sulla protezione dei dati") qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
 - (ii) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento

presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

- (iii) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
 - (iv) gli obblighi di cui all'articolo 32 del RGPD.
- (d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9 - Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del RGPD, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1 Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

- (a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
- (b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del RGPD, devono essere indicate nella notifica del titolare del trattamento e includere almeno:
 - (i) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - (ii) le probabili conseguenze della violazione dei dati personali;
 - (iii) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

- (c) nell'adempire, in conformità dell'articolo 34 del RGPD all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2 Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

- (a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
- (b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
- (c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del RGPD.

SEZIONE III
-
DISPOSIZIONI FINALI

Clausola 10 - Inosservanza delle clausole e risoluzione

- (a) Fatte salve le disposizioni del RGPD, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.
 - (b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:
 - (i) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
 - (ii) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del RGPD;
 - (iii) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del RGPD.
 - (c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.
 - (d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.
-

ALLEGATO I

-

ELENCO DELLE PARTI

Titolare del trattamento

Il Cliente, come identificato mediante login alla piattaforma.

Modalità di adesione e sottoscrizione del presente DPA: Il Cliente accetta e sottoscrive il presente atto con il c.d. metodo "point and click" selezionando con il proprio cursore l'apposita casella relativa al DPA prevista in fase di primo accesso all'account fornito in seguito alla sottoscrizione del Contratto principale. Il Cliente potrà trovare una copia aggiornata del presente atto all'interno del proprio account nella pagina del Profilo.

Develop-Players S.r.l. per finalità legate alla sottoscrizione e all'adempimento del presente contratto, conserverà il log contenente la data e l'ora dell'accettazione del DPA da parte del Cliente con il metodo point and click. In caso di modifiche importanti al presente documento, Develop-Players S.r.l. potrà chiedere al Cliente di accettare le nuove condizioni con la stessa modalità.

Responsabile del Trattamento

Nome: Develop-Players S.r.l.

Indirizzo: Via Passo Corelli 35, 47522, Cesena (FC) - Italia

Contatti:

Amministratore Delegato

luca.formica@develop-players.com

Firma:



ALLEGATO II

-

DESCRIZIONE DEL TRATTAMENTO

II.1. - Finalità del trattamento, categorie di interessati e dati trattati da parte del Responsabile del trattamento per conto del Titolare del trattamento

La finalità del trattamento è la fornitura del nostro servizio e le funzionalità in essa contenute come descritte nei Termini e Condizioni in cui il presente DPA è allegato.

Per le funzionalità base:

Attività	Interessato	Categorie di dati personali	Categoria speciale di dati	Esempi di dati trattati
Funzionalità "invita familiare" Il clinico può inserire l'indirizzo email di un familiare e invitarlo ad accedere alla piattaforma e seguire i progressi del paziente.	Develop-Players User - Customer	Identificativi Informazioni Personali	No	Email
Funzionalità di valutazione, gestione trattamenti, training, prescrizioni e anagrafica Permettere ai clinici di svolgere le proprie attività professionali, per finalità di cura dei propri pazienti, avvalendosi delle funzionalità della piattaforma. I dati sono conservati su AWS.	Develop-Players - Paziente	Dati comuni Caratteristiche personali	No	Sesso
		Dati comuni - Sfera familiare e abitativa	No	- CAP - Città
		Identificativi Informazioni Personali	No	- Codice Fiscale (C.F.) - Cognome - Data di nascita - Informazioni di contatto principali - Informazioni di contatto secondarie - Nome
		Dati relativi alla salute	Sì	- Altra diagnosi - Checkpoint (test) giocati dal paziente - Criteri di selezione del clinico - Dettagli potenziamento - Diagnosi principale - Diario clinico del trattamento del paziente - Giocate completate dal paziente - Note del professionista - Prescrizioni per la famiglia - Professionista sanitario - Relazioni esami clinici - Stato clinico - Valutazioni cliniche
Salvataggio sessioni di gioco completate Per permettere al clinico di svolgere le attività di diagnosi e cura, la piattaforma conserva i dati rilevanti relativi ai checkpoint raggiunti e alle giocate completate dal paziente ai videogiochi di	Develop-Players - Paziente	Identificativi Informazioni Personali	No	- Codice Fiscale (C.F.) - Cognome - Data di nascita - Età - Informazioni di contatto principali - Informazioni di contatto secondarie - Nome

Attività	Interessato	Categorie di dati personali	Categoria speciale di dati	Esempi di dati trattati
Screening, Valutazione e Trattamento.				• Provincia di residenza
		Dati relativi alla salute	Sì	• Checkpoint (test) giocati dal paziente • Giocate completate dal paziente

Per le funzionalità IA:

Attività	Interessato	Categorie di dati personali	Categoria speciale di dati	Esempi di dati trattati
Funzionalità IA La piattaforma permette al professionista di utilizzare l'IA avanzata per commentare test clinici, relazioni cliniche e per il caricamento e analisi di documenti clinici che l'utente può caricare in piattaforma.	Develop-Players - Paziente	Dati comuni - Caratteristiche personali	No	• Sesso
		Dati comuni - Sfera familiare e abitativa	No	• CAP • Città
		Identificativi - Informazioni Personali	No	• Codice Fiscale (C.F.) • Cognome • Data di nascita • Età • Informazioni di contatto principali • Informazioni di contatto secondarie • Nome • Provincia di residenza
		Dati relativi alla salute	Sì	• Altra diagnosi • Contesto in cui emergono le difficoltà principali • Criteri di selezione del clinico • Dettagli potenziamento • Diagnosi derivanti dalle giocate completate dal paziente • Diagnosi principale • Diario clinico del trattamento del paziente • Difficoltà riscontrate o sospettate • Eventuali precedenti diagnosi (es. ADHD, DSA) • Note del professionista • Periodo di tempo da quando si sono presentate queste difficoltà • Predisposizione a intraprendere un percorso di supporto • Prescrizioni per la famiglia • Professionista sanitario • Relazioni esami clinici • Scopo di un confronto con uno psicologo • Stato clinico • Strumenti o percorsi di supporto eventualmente già provati • Valutazioni cliniche

II.2. Il trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare ha la seguente durata e frequenza:

La durata e la frequenza del trattamento sarà la stessa del Contratto stipulato tra le parti.

II.3. Altre disposizioni in merito al trattamento dei dati personali degli Utenti e del Titolare del trattamento.

Per quanto attiene i trattamenti di dati personali e di categorie particolari di dati personali necessari per le finalità di cura e oggetto del presente documento, il titolare del trattamento rimane il Professionista che deve, quindi, fornire una propria apposita informativa privacy al paziente in cui Develop-Players S.r.l. risulta tra i responsabili del trattamento in virtù del presente accordo. Laddove il Professionista volesse avvalersi delle funzionalità di IA messe a disposizione dalla piattaforma per analizzare l'esito delle giocate del paziente e/o per semplificare la redazione di documentazione medica (es. relazioni), lo stesso dovrà informare gli interessati anche di tale trattamento ed eventualmente, se necessario, raccogliere i consensi per tali tipologie di trattamento dei dati personali.

ALLEGATO III

MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

[Azienda] Develop-Players S.r.l.

Misure di Sicurezza Organizzative

Documentazione

[Azienda] Develop-Players S.r.l.

L'azienda dispone di un elenco interno di tutte le informative sulla privacy in vigore.

Ruoli e responsabilità in materia di privacy

[Azienda] Develop-Players S.r.l.

La RPD è stata designata sulla base delle qualità professionali e delle conoscenze specialistiche. I dati di contatto della RPD sono stati comunicati all'Autorità Garante per la protezione dei dati personali competente.

La RPD è coinvolta in modo adeguato e tempestivo nelle questioni relative alla protezione dei dati.

Alla RPD vengono fornite le risorse necessarie e l'accesso ai dati personali e alle operazioni di trattamento per l'esecuzione dei propri compiti e il mantenimento delle conoscenze.

L'azienda garantisce l'indipendenza della RPD dalle istruzioni e dalle conseguenze per l'esecuzione dei compiti.

La RPD risponde direttamente al livello dirigenziale più alto dell'azienda.

Vengono adottate misure per prevenire conflitti di interesse qualora la RPD svolga compiti aggiuntivi.

The company has planned to appoint Chino S.r.l. as external DPO.

Gli interessati possono contattare la RPD in merito ai propri dati personali e ai propri diritti previsti dal GDPR.

Pianificazione e preparazione per la sicurezza

Continuità operativa aziendale

[Azienda] Develop-Players S.r.l.

The Company has performed a Business Impact Analysis, following ISO 27001 best practices.

Gli RTO sono stati definiti e testati dall'Azienda.

Gli RPO sono stati definiti e testati dall'azienda.

Gestione delle risorse

[Azienda] Develop-Players S.r.l.

L'azienda dispone di un registro di tutte le risorse IT coinvolte nella soluzione.

Misure di sicurezza interna

[Azienda] Develop-Players S.r.l.

L'Azienda consente il trasferimento, l'archiviazione o qualsiasi trattamento di dati protetti o informazioni sensibili al di fuori dei locali dell'organizzazione o su dispositivi mobili e ha attuato una politica per regolamentare l'uso di dispositivi esterni o rimovibili, di proprietà dell'azienda o del personale ("Bring Your Own Device - BYOD").

I computer portatili e le postazioni di lavoro si bloccano automaticamente dopo un certo periodo di tempo.

L'azienda protegge tutti i dispositivi interni e le postazioni di lavoro con soluzioni e procedure anti-malware e di monitoraggio delle vulnerabilità.

Tutte le risorse che trattano dati protetti sono crittografate.

Consapevolezza, istruzione e formazione sulla sicurezza informatica

[Azienda] Develop-Players S.r.l.

L'azienda dispone di un registro delle violazioni dei dati contenente i dati e i dettagli delle violazioni dei dati, nonché le azioni di mitigazione intraprese.

Sicurezza fisica e ambientale

[Azienda] Develop-Players S.r.l.

The Company has implemented contingency operations for its physical premises.
L'azienda ha una "Politica di sicurezza fisica e ambientale".

[Azienda] Develop-Players S.r.l.

L'azienda protegge tutti i dispositivi interni e le postazioni di lavoro con firewall.

[Prodotto] Develop-Players

Misure di Sicurezza Organizzative

Documentazione

[Prodotto] Develop-Players

Il RoPA per le attività svolte in qualità di Titolare contiene tutte le informazioni ai sensi dell'art. 30 GDPR relative al Progetto analizzato.

Il RoPA per le attività svolte in qualità di Responsabile del trattamento contiene tutti i requisiti obbligatori ai sensi dell'art. 30 GDPR.

[Prodotto] Develop-Players

L'azienda raccoglie il consenso degli interessati per le attività che svolge sulla base del Consenso.

La richiesta di consenso è chiaramente distinguibile dalle altre questioni, presentata in una forma intelligibile e facilmente accessibile, e utilizza un linguaggio chiaro e semplice in conformità con l'art. 7 del GDPR.

Gli individui vengono adeguatamente informati prima di dare il consenso.

Nel caso in cui i dati non siano necessari per l'erogazione del servizio, il consenso è facoltativo (liberamente prestato).

Gli interessati possono revocare il proprio consenso in qualsiasi momento.

Il sistema per revocare il consenso è facilmente accessibile agli interessati.

[Interessato] Develop-Players User - Customer

Tutte le comunicazioni con gli interessati sono concise, intelligibili, facilmente accessibili e utilizzano un linguaggio chiaro e semplice.

[Interessato] Develop-Players - Paziente

L'azienda ha già reso disponibile un'informativa sulla privacy per il progetto per questo interessato.

L'Informativa sulla privacy è accessibile e liberamente consultabile in qualsiasi momento.

L'informativa sulla privacy contiene tutte le informazioni necessarie, tra cui: Le finalità del trattamento; La base giuridica del trattamento; L'identità del titolare del trattamento; I dati di contatto del titolare del trattamento; I dati di contatto del Responsabile del trattamento dei dati (se applicabile); I destinatari o le categorie di destinatari dei dati personali; Le categorie di dati personali trattati; I periodi di conservazione dei dati personali oppure, ove ciò non sia possibile, i criteri utilizzati per determinare tale periodo; Il diritto di richiedere l'accesso, la cancellazione, la rettifica, la limitazione, l'opposizione e la portabilità dei dati personali; Il diritto di revocare il consenso in qualsiasi momento (se il trattamento è basato sul consenso); Il diritto di proporre reclamo a un'autorità di protezione dei dati; L'esistenza di un processo decisionale automatizzato e informazioni pertinenti sulla logica sottostante e sulle conseguenze previste del trattamento per l'interessato.

Tutte le comunicazioni con gli interessati sono concise, intelligibili, facilmente accessibili e utilizzano un linguaggio chiaro e semplice.

[Prodotto] Develop-Players

L'azienda ha effettuato e documentato un'analisi strutturata dei rischi per la sicurezza delle informazioni relativi al proprio prodotto, considerando diversi scenari di minaccia e l'intera catena di fornitura, e definendo le misure di sicurezza appropriate per mitigare tali rischi.

L'Azienda ha valutato adeguatamente i requisiti di ridondanza dei componenti e dei sistemi del prodotto.

I sistemi di ridondanza implementati soddisfano i requisiti del prodotto al fine di garantire la disponibilità e l'integrità delle informazioni.

L'azienda impiega reti ridondanti per i servizi di produzione.

[Destinatario dei dati] Clinico

Il DPA standard copre tutti i requisiti obbligatori.

Misure di Sicurezza Informatiche

Controlli informatici

Crittografia di rete

[Prodotto] Develop-Players

Tutte le comunicazioni tra l'applicazione e il backend crittografate utilizzano almeno TLS 1.3.

In caso di trasferimento di dati protetti a provider esterni, l'azienda ne garantisce la crittografia durante il transito.

Sicurezza degli endpoint

[Prodotto] Develop-Players

L'azienda garantisce che gli URL delle API non contengano mai informazioni sensibili, come chiavi API e token di sessione.

Controllo di sicurezza del sistema IT

[Prodotto] Develop-Players

Tutti gli account utente e ospiti predefiniti sono stati rimossi dal backend e dai sistemi interni.

Tutte le applicazioni e i driver non necessari installati per default sono stati rimossi dai sistemi interni e dal backend.

Tutti i servizi non necessari sui server e sui sistemi backend sono stati bloccati o eliminati.

Tutti i server sono aggiornati e sottoposti a patch regolarmente.

L'autenticazione dell'applicazione è gestita nel backend.

È stata implementata la sincronizzazione degli orologi di sistema da un'unica sorgente oraria condivisa verificata.

L'applicazione verifica l'autenticità dei servizi richiamabili tramite rete aperta prima che vengano scambiati dati personali con essi.

Messages and data sent via open networks to the application services are checked against defined schemes and known attack vectors.

L'azienda mantiene attivi solo i metodi di autenticazione necessari per i servizi richiamati tramite rete aperta.

L'Azienda ha una procedura in atto per assegnare le autorizzazioni di accesso in modo restrittivo per impostazione predefinita.

Gestione dello sviluppo

[Prodotto] Develop-Players

The Company uses developer tools that allow to control access and changes to the code base (GitHub).

L'azienda garantisce l'utilizzo di password complesse per l'accesso a tutti gli strumenti di sviluppo software e al codice base.

The Company ensures that all passwords for 3rd party provider logins that have access to the source code repository or personal data repository are adequately strong.

The Company maintains an accurate log of all accesses to the source code repository.

Code Read and Write privileges are strictly assigned to authorised personnel who need access to perform their task.

The development tools used by the Company allow for proper control on changes to the code.

The Company maintains an accurate change log for all source code updates.

L'azienda mantiene un elenco completo di tutte le librerie e dei software di terze parti utilizzati nello sviluppo.

The Company ensures that the application developed, and any following updates, are sufficiently tested, in a manner that simulates real use, before they are pushed into production.

For testing, the Company ensures the following: Testing is clearly planned and scheduled; Inputs and expected outputs are clearly defined; Testing results are measured against set evaluation criteria; Testing is performed at least in two steps, by the development team and then by an independent



acceptance team; Testing conditions match Production environment conditions as closely as possible; Testing schedule includes time for feedback, remedial actions implementation and re-testing. The Company enforces the separation of environments between development, testing, and production. The Company ensures that protected/sensitive data is never copied or used outside production environments.

Qualità del codice

[Prodotto] Develop-Players

L'azienda esamina regolarmente tutto il codice per individuare eventuali bug.
L'azienda utilizza strumenti automatizzati per la revisione del codice.
Tutto il codice dello sviluppatore viene rimosso dall'applicazione prima del rilascio.
Il codice viene attivamente offuscato per prevenire attacchi come il reverse engineering.
Il codice viene controllato per individuare errori normali ed eccezionali.

Controlli di sicurezza delle applicazioni

[Prodotto] Develop-Players

L'azienda garantisce che l'applicazione impedisca attacchi da parte di strumenti di debugger o di reverse engineering.
L'applicazione è in grado di rilevare se c'è un tentativo esterno di accedere o modificare il codice e i dati nel suo spazio di memoria.
Gli errori generati da voci di database errate o casi di uso improprio vengono esclusi o gestiti in modo predefinito.
I dati sono codificati in un formato che garantisce che il codice malevolo non venga interpretato o eseguito, impedendo l'iniezione di codice.
Vengono fatti dei controlli per password e backdoor incorporate sulla versione di produzione dell'applicazione.
L'applicazione utilizza certificati sicuri propri o certificati firmati da un'autorità di certificazione verificata come attendibile.
L'azienda garantisce la sostituzione dei certificati alla loro scadenza.
Tutti i file di configurazione rilevanti dell'applicazione sono protetti contro la perdita e la falsificazione mediante misure tecniche adeguate.

Sicurezza IT dell'applicazione

[Prodotto] Develop-Players

L'azienda assicura che nessuna credenziale venga memorizzata nel codice sorgente in alcun formato.
Any cache and any temporary data is regularly deleted after the user session termination.
L'azienda assicura che nessun dato protetto venga archiviato all'esterno del contenitore dell'app.
L'azienda garantisce che i messaggi di errore non rivelino dati protetti o riservati.

Distribuzione delle applicazioni

[Prodotto] Develop-Players

L'applicazione funziona solo sulle versioni correnti del sistema operativo/browser ancora supportate dal dispositivo o dal produttore.

Controllo degli accessi alle infrastrutture

[Componente Architetture] AWS Auth

L'Azienda limita e controlla l'uso di programmi di utility privilegiati, consentendone l'utilizzo sui sistemi solo agli utenti autorizzati.
All instances of privileged actions and applications are properly logged in CloudTrail.
Gli accessi come superuser, root, con privilegi o admin sono limitati in modo specifico.
The Company properly tracks the authorisation levels of privileged utility programs, including the assigned account, role and user for each level.
L'azienda assegna gli account con privilegi a individui specifici e identificabili.
The Company ensures that privileged environments/modes are logically segregated and clearly distinguishable from normal production environment/mode.



Gestione dell'autenticazione

[Componente Architetturale] [F] User's Login

L'Azienda impone l'autenticazione per tutti i dati non pubblici.

The Company enforces user authentication with an appropriate level of security.

Tutti i dati di autenticazione degli utenti vengono conservati in modo sicuro.

L'azienda testa i flussi di accesso, assicurandosi che l'autenticazione e l'autorizzazione vengano eseguite correttamente.

[Componente Architetturale] AWS Auth

L'Azienda impone l'autenticazione per tutti i dati non pubblici.

The Company enforces user authentication with an appropriate level of security.

Tutti i dati di autenticazione degli utenti admin vengono conservati in modo sicuro.

L'azienda testa i flussi di accesso, assicurandosi che l'autenticazione e l'autorizzazione vengano eseguite correttamente.

Gestione della sessione

[Componente Architetturale] [F] User's Login

Il backend/endpoint API genera identificatori di sessione casuali con entropia sufficiente e tramite procedure stabilite.

Il token viene firmato utilizzando un algoritmo sicuro.

Le sessioni utente terminano automaticamente dopo un intervallo di tempo definito o dopo un periodo di inattività dell'utente.

È garantito che una sessione una volta invalidata non possa essere riattivata anche se sono noti i dati della singola sessione.

L'Azienda garantisce che l'utente possa uscire dalla sessione e invalidarla esplicitamente.

[Componente Architetturale] AWS Auth

Le sessioni amministrative terminano automaticamente dopo un intervallo di tempo definito.

Autenticazione a più fattori (MFA)

[Componente Architetturale] [F] User's Login

L'Azienda ha attuato l'autenticazione a più fattori.

L'Azienda garantisce che l'utente possa attivare l'autenticazione a più fattori in qualsiasi momento all'interno dell'applicazione.

[Componente Architetturale] AWS Auth

L'Azienda ha attuato l'autenticazione a più fattori.

Diritti di accesso all'applicazione e login

[Componente Architetturale] [F] User's Login

L'Azienda garantisce che gli utenti dispongano di diritti di accesso e permessi in linea con le loro attività e ruoli, nel rispetto dei principi di "need-to-know" e di "minimo privilegio".

Ogni utente ha un identificativo di accesso univoco.

L'Azienda dispone di una procedura formale per l'assegnazione e la revoca dei privilegi a un utente.

[Componente Architetturale] AWS Auth

L'Azienda garantisce che gli utenti dispongano di diritti di accesso e permessi in linea con le loro attività e ruoli, nel rispetto dei principi di "need-to-know" e di "minimo privilegio".

Ogni utente ha un identificativo di accesso univoco.

L'Azienda dispone di una procedura formale per l'assegnazione e la revoca dei privilegi a un utente.

Gestione delle password

[Componente Architetturale] [F] User's Login

L'applicazione impone l'uso di una password o PIN per accedervi.

I requisiti minimi di complessità delle password sono sufficientemente elevati da garantire un adeguato livello di sicurezza.

L'Applicazione è protetta dall'accesso automatizzato mediante adeguati meccanismi di protezione.



La procedura di modifica della password richiede l'utilizzo della vecchia password o di un altro metodo per verificare l'identità dell'utente.

Viene garantito che le password non vengano mai trasmesse o memorizzate in chiaro.

Il testo nelle caselle di inserimento di password viene oscurato usando asterischi o simili.

La copia del testo dalle caselle di inserimento password viene impedita.

[Componente Architettuale] AWS Auth

L'applicazione impone l'uso di una password o PIN per accedervi.

The re-use of previous passwords by users is prevented.

Viene garantito che le password non vengano mai trasmesse o memorizzate in chiaro.

Il testo nelle caselle di inserimento di password viene oscurato usando asterischi o simili.

La copia del testo dalle caselle di inserimento password viene impedita.

L'Azienda registra nel sistema la modifica o la reimpostazione delle password.

Errori di accesso e avvisi

[Componente Architettuale] [F] User's Login

Tutti gli errori o malfunzionamenti del sistema di controllo degli accessi comportano il rifiuto dell'accesso.

Crittografia dei dati

[Componente Architettuale] [DB] AWS RDS for PostgreSQL

Tutti i dati sensibili e personali trattati dall'applicazione vengono crittografati.

L'Azienda ha il controllo diretto delle procedure relative alla gestione delle chiavi crittografiche.

Attualmente le chiavi crittografiche vengono archiviate su sistemi diversi dai dati sensibili.

[Componente Architettuale] AWS Auth

Tutti i dati sensibili e personali trattati dall'applicazione vengono crittografati.

L'Azienda ha il controllo diretto delle procedure relative alla gestione delle chiavi crittografiche.

Attualmente le chiavi crittografiche vengono archiviate su sistemi diversi dai dati sensibili.

[Componente Architettuale] [DB] AWS S3

Tutti i dati sensibili e personali trattati dall'applicazione vengono crittografati.

L'Azienda ha il controllo diretto delle procedure relative alla gestione delle chiavi crittografiche.

Attualmente le chiavi crittografiche vengono archiviate su sistemi diversi dai dati sensibili.

Minimizzazione dei dati

[Prodotto] Develop-Players

L'applicazione prevede fin dalla progettazione la minimizzazione dei dati personali.

L'Azienda si assicura di ridurre al minimo le duplicazioni inutili di dati all'interno dei sistemi.

Qualità e integrità dei dati

[Prodotto] Develop-Players

L'Azienda definisce la classificazione delle informazioni in base alla sensibilità, criticità, riservatezza, requisiti di privacy e valore delle informazioni.

The system also allows access to public data and the Company ensures that access to public data is physically and logically segregated from sensitive/protected data.

L'Azienda convalida il formato, la correttezza e la completezza di tutti i dati raccolti.

L'Azienda impiega meccanismi per garantire l'integrità dei dati archiviati.

Viene garantito che tutti gli aggiornamenti dei dati vengano immediatamente propagati a tutti i sistemi che ne hanno bisogno.

Cancellazione dei dati

[Componente Architettuale] [DB] AWS RDS for PostgreSQL

L'Azienda ha una procedura per garantire che tutti i dati vengano eliminati dalle apparecchiature non più utilizzate per il progetto.

L'Azienda ha definito tempi massimi di conservazione per tutte le tipologie di dati trattati, compresi i backup.

Tutti i dati personali vengono cancellati automaticamente dopo un periodo di tempo definito.



L'Azienda ha implementato un meccanismo per cancellare automaticamente i dati una volta raggiunto il tempo massimo di conservazione.

Tutte le copie di backup vengono cancellate automaticamente dopo un periodo di tempo definito.

[Componente Architetture] AWS Auth

L'Azienda ha definito tempi massimi di conservazione per tutte le tipologie di dati trattati, compresi i backup.

Tutte le copie di backup vengono cancellate automaticamente dopo un periodo di tempo definito.

[Componente Architetture] [DB] AWS S3

L'Azienda ha una procedura per garantire che tutti i dati vengano eliminati dalle apparecchiature non più utilizzate per il progetto.

Backup

[Componente Architetture] [DB] AWS RDS for PostgreSQL

The Company performs backups of all protected data processed in the system.

The Company performs backups of all authentication data stored by the system.

The Company performs backups of all encryption keys stored by the system.

The frequency of backups is defined and formally documented and is adequate for the system recovery needs.

I backup vengono eseguiti con uno strumento automatico.

I backup vengono conservati in modo sicuro, in un formato crittografato.

The Company implements mechanisms to ensure the integrity and completeness of the backups as they are created.

I backup si trovano in una posizione fisica diversa rispetto ai server primari.

For the backup sites, the Company applies the same level of security of its main sites.

[Componente Architetture] AWS Auth

The Company performs backups of all protected data processed in the system.

The Company performs backups of all authentication data stored by the system.

The Company performs backups of all encryption keys stored by the system.

The frequency of backups is defined and formally documented and is adequate for the system recovery needs.

I backup vengono conservati in modo sicuro, in un formato crittografato.

The Company implements mechanisms to ensure the integrity and completeness of the backups as they are created.

I backup si trovano in una posizione fisica diversa rispetto ai server primari.

For the backup sites, the Company applies the same level of security of its main sites.

[Componente Architetture] [DB] AWS S3

The Company performs backups of all authentication data stored by the system.

The Company performs backups of all encryption keys stored by the system.

Sistema di log

[Componente Architetture] AWS Auth

The Company has implemented a system for logging all data operations.

Il sistema di logging genera registri di controllo adeguati, contenenti tutte le informazioni necessarie per comprendere la cronologia delle operazioni eseguite sui dati personali.

Vengono registrate tutte le attività svolte dagli amministratori, dai superuser e dagli altri account con accesso privilegiato.

[Componente Architetture] [DB] AWS S3

L'Azienda dispone di un sistema per il logging di tutte le operazioni sui dati.

Il sistema di logging genera registri di controllo adeguati, contenenti tutte le informazioni necessarie per comprendere la cronologia delle operazioni eseguite sui dati personali.

Vengono registrate tutte le attività svolte dagli amministratori, dai superuser e dagli altri account con accesso privilegiato.

L'accesso al sistema di tracciamento è limitato solo al personale autorizzato.

Il sistema di tracciamento è in grado di verificare l'integrità dei registri.

[Componente Architetture] [F] User's Login

L'accesso al sistema di tracciamento è limitato solo al personale autorizzato.

Il sistema di tracciamento è in grado di verificare l'integrità dei registri.

[Componente Architetture] [DB] AWS RDS for PostgreSQL

L'accesso al sistema di tracciamento è limitato solo al personale autorizzato.

Gestione dei log

[Prodotto] Develop-Players

I logs sono raccolti in un sistema centrale (AWS Cloudwatch).

L'Azienda garantisce che i logs non contengano dati personali.

Logs are protected against unauthorised editing, deletion or tampering.

Terze parti - Controlli tecnici

Standard di sicurezza dichiarato

[Destinatario dei dati] Amazon Web Services EMEA SARL

L'azienda verifica che il fornitore dei servizi cloud implementi una protezione contro malware, DDoS e altre forme di traffico indesiderato.

L'azienda verifica che il fornitore di servizi cloud fornisca garanzie scritte riguardo alla protezione da accessi non autorizzati al data centre.

Livello di servizio

[Destinatario dei dati] Amazon Web Services EMEA SARL

L'azienda verifica se gli SLA/MSA/BAA indicati nei contratti con i fornitori terzi soddisfano le sue esigenze operative.

The security controls guaranteed by the provider are sufficient for security needs of the Company.

I fornitori terzi garantiscono che i dati personali verranno eliminati definitivamente dagli stessi e dai loro sub-responsabili al momento della cessazione del servizio o su richiesta diretta.

Continuità aziendale di terze parti

[Destinatario dei dati] Amazon Web Services EMEA SARL

L'azienda ha accesso a una copia dei piani di Ripristino in caso di emergenza dei fornitori terzi utilizzati per la soluzione software.

Gli RTO e RPO (Recovery Time Objective e Recovery Point Objective) del fornitore sono in linea con le esigenze dell'applicazione.

ALLEGATO IV

-

ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

Per le funzionalità base:

(Sub)responsabili	Luoghi del trattamento	Attività	Interessato	Categoria di dati
Amazon Web Services EMEA SARL	EEA (Area Economica Europea)	Funzionalità di valutazione, gestione trattamenti, training, prescrizioni e anagrafica	Develop-Players - Paziente	Dati comuni - Caratteristiche personali
				Dati comuni - Sfera familiare e abitativa
				Identificativi - Informazioni Personali
				Dati relativi alla salute
Polarity S.r.l.	EEA (Area Economica Europea)	Funzionalità di valutazione, gestione trattamenti, training, prescrizioni e anagrafica	Develop-Players - Paziente	Dati comuni - Caratteristiche personali
				Dati comuni - Sfera familiare e abitativa
				Identificativi - Informazioni Personali
				Dati relativi alla salute

Per le funzionalità IA:

(Sub)responsabili	Luoghi del trattamento	Attività	Interessato	Categoria di dati
Amazon Web Services EMEA SARL	EEA (Area Economica Europea)	Funzionalità IA	Develop-Players - Paziente	Dati comuni - Caratteristiche personali
				Dati comuni - Sfera familiare e abitativa
				Identificativi - Informazioni Personali
				Dati relativi alla salute